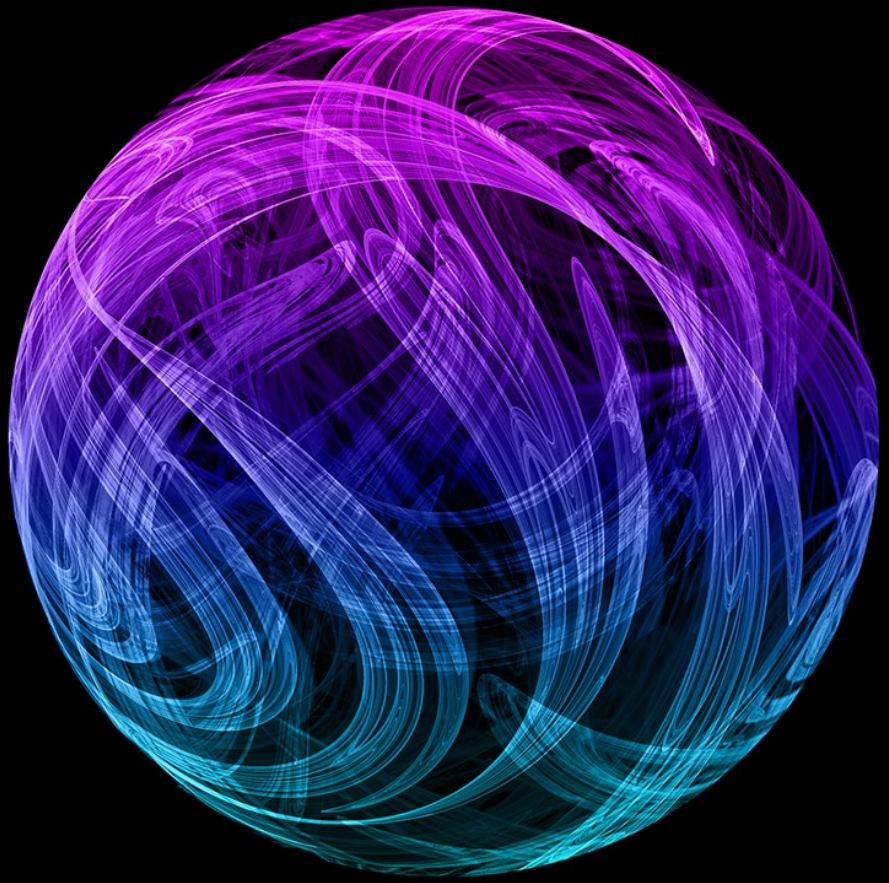
Deloitte.



Internal audit planning priorities 2025

Financial Services

Banking and capital markets

MAKING AN IMPACT THAT MATTERS since 1845

Executive summary

Celebrating 10 years of planning priorities

Welcome to Deloitte's Financial Services planning priorities for internal audit for 2025.

As we launch the 10th edition of this publication, we recognise the pivotal role internal audit continues to play. Internal audit is the backbone supporting organisations on their journey forward, acting as a strategic partner and providing insight and innovation for organisations to thrive today and in the future.

The Financial Services landscape in 2024 continues to be driven by increasing regulation, which is impacting many firms' cost-base due to the need for more robust and well controlled processes. This is compounded by wider economic volatility stemming from ongoing global conflicts, a higher interest rate environment and elections taking place across 70 countries worldwide, including in the UK.

Despite the uncertainty this brings, the role of internal audit as a strategic partner remains unchanged, and many of the key topics for functions to consider today are common with those highlighted in the first edition of this publication in 2014, including model risk management, third party risk management and financial crime. This is perhaps unsurprising given that regulatory focus remain largely the same, centred on prudential stability, good customer outcomes and the reduction and prevention of financial crime.

Whilst similarities remain, internal audit functions must continue to evolve to keep pace with change, not just in terms of what they audit but how they audit. Generative AI (GenAI) in particular presents huge opportunities with a significant increase in the number of use cases emerging across the last 12 months, both in terms of how firms use GenAI, as well as how functions can benefit from it.

This year's publication reflects a continued focus on prudential risk and incoming regulations including Basel 3.1, the Small Domestic Deposit Takers regime and solvent exit planning, as well as liquidity and model risk considerations amongst others.

For the second year, we have a section dedicated to environmental, social, and governance (ESG). With notable increases in the quantity, quality and breadth of reporting and disclosures due over this and coming years, driven by regulations such as the Corporate Sustainability Reporting Directive (CSRD), ESG continues to be a focus area. Regulation aside, firms should be mindful of the strategic decisions required to effect change as well as report accurately.

The focus on financial crime, conduct risk and digital risk continues. There are also a number of new focus areas to consider including in annual audit plans. An increase in the volume and quantity of financial penalties resulting from failures to correctly identify off-payroll workers has brought employment taxes into focus. Regulators are also focusing on motor finance discretionary commission, which has also been included.

The banking industry is a dynamic and critical sector, constantly facing evolving risks that demand robust internal audit and risk management practices. In this modern financial landscape, internal audit is instrumental in safeguarding the stability and integrity of the sector.

Navigate through the topics that follow and are most relevant to you and your organisation for an overview and suggested actions on a range of priorities for 2025. These are intended to provide a useful reference point from which to drive conversations and ultimately help define internal audit plans.

We hope you find the topics useful and if you would like to discuss anything further, please get in touch.

Aaron Oxborough
Partner
aoxborough@deloitte.co.uk

Russell Davis
Partner
rdavis@deloitte.co.uk

Matt Cheetham
Partner
mcheetham@deloitte.co.uk

Louise Roberts
Senior Manager
louiseroberts@deloitte.co.uk

Table of contents

New regulation and emerging risk

Small Domestic Deposit Taker regime

Solvent exit planning

Regulatory issue validation

Basel 3.1

Employment taxes

01

New regulation and emerging risk

Small Domestic Deposit Taker regime

In January 2024, the Prudential Regulation Authority (PRA) finalised its policy on the operation of the Small Domestic Deposit Taker (SDDT) regime. Banks and building societies that meet the SDDT criteria are now able to apply to the PRA to enter the regime and be in scope for a simpler set of prudential rules and requirements. Currently, simpler rules have been defined for liquidity and Pillar III disclosures and we expect that the PRA will consult on simpler capital rules in Q3 2024.

Four things you should know

- Firms can apply for entry to the SDDT regime by taking up the PRA's offer of an application to become subject to SDDT rules. Application criteria centres around total asset size, domestic activity, limited trading activity, amongst others (full list here). Note that, the PRA can revoke a firm's SDDT designation if eligibility criteria is subsequently breached, and if revoked, the firm should prepare to operate under non-SDDT prudential rules immediately.
- Although firms with foreign parents are not eligible for the SDDT regime, the PRA considers that such firms may be treated as SDDT-eligible if they satisfy all other SDDT criteria, and where total group assets do not exceed £20bn. The PRA will consider these applications on a case-by-case basis.
- Currently, firms that have an approved modification by consent are in scope for several areas of simplified prudential rules and guidance:
  - **Internal Liquidity Adequacy Assessment Process (ILAAP):** SDDT firms can submit a simplified ILAAP. The PRA published a template and guidance in its updated SS24/15 document.
  - **Pillar two liquidity:** The PRA considers that SDDT firms are unlikely to run Pillar two risks that are material compared to their Pillar one risks. It therefore proposes to not apply Pillar 2 liquidity guidance to SDDT Firms with limited exceptions.
  - **Retail Deposit Ratio:** A new Retail Deposit Ratio (RDR) will be used to measure firms' usage of retail funding. This is calculated as a ratio of total retail deposits to total funding. Where firms meet a four-quarter moving average for the RDR of ≥50%, the PRA will disapply NSFR reporting requirements.
  - **Liquidity reporting:** SDDT firms are excluded from reporting four of the five Additional Liquidity Monitoring Metrics (ALMM) returns. Concentration by product type (c68) will continue to be reported by SDDT firms, and SDDTs will be required to report all relevant product types, rather than just those that comprise greater than 1% of their total liabilities as at present.
  - **Pillar three:** Small and non-complex (SNCI) firms, with listed financial instruments, who go onto achieve SDDT status, are eligible for a reduced set of disclosure requirements. Non-listed SNCI firms who achieve SDDT status are exempt from all Pillar three disclosure requirements.
- Whilst the PRA focuses on the simplified regime for capital requirements, SDDT firms do not have to apply Basel 3.1 standards at the implementation date. Instead, they can enter a "Transitional Capital Regime" based on current Capital Requirement Regulation (CRR) provisions until the simplified capital regime for SDDT firms comes into force.

Four things internal audit should do

1. **Monitoring SDDT criteria**
   Internal audit should consider reviewing how management plans to monitor criteria for the application of SDDT on an ongoing basis, including a set of triggers to monitor and the actions to be taken before an eligibility criteria breach occurs.
2. **ILAAP**
   Internal audit should review their firms existing ILAAP against all aspects of the simplified ILAAP template to provide assurance that firm-specific risks have been covered in a proportionate manner.
3. **Retail Deposit Ratio (RDR)**
   Internal audit should consider the controls in place to ensure accurate reporting and monitoring of the RDR ratio, ensuring appropriate action can be taken before the RDR reaches the threshold level.
4. **Additional liquidity monitoring metrics (ALMM) c68 template**
   Internal audit should review the process and controls inherent in the ALMM reporting process to ensure the c68 is being reported in line with the new guidance.

To discuss this topic further, please get in touch.

Sinead Rothwell
Partner
srothwell@deloitte.co.uk

Amarit Bains
Senior manager
amaritbains@deloitte.co.uk

01

New regulation and emerging risk

Solvent exit planning

In March 2024, the Prudential Regulation Authority (PRA) finalised its policy on solvent exit planning, which is largely unchanged from the 2023 consultation paper and is relevant to non-systemic UK banks and building societies. Regulations are due to come into force in Q3 2025. A solvent exit means the process through which a firm ceases PRA-regulated activities (deposit-taking), while remaining solvent throughout to the point that they can be liquidated safely and repay all depositors and creditors in full, or continue as a Financial Conduct Authority (FCA) solo-regulated entity. The firm should transfer or repay (or both) all deposits as part of its solvent exit. Once the firm has transferred and/or returned all deposits, a solvent exit will end with the removal of the firm's Part 4A PRA permission.

Five things you should know

- The supervisory statement lays out the following as areas that must be covered by solvent exit analysis (SEA) in a "proportionate" level of detail: solvent exit actions; solvent exit indicators; potential barriers and risks; resources and costs; communication; governance and decision-making; and assurance.
- If a solvent exit becomes likely, the firm must prepare a solvent exit execution plan (SEEP). The SEEP will need to be prepared quickly, likely within a month.
- There should be a well-evidenced approach to selecting indicators and their calibration. In calibrating trigger points, the SEA needs to show that there is sufficient time post-trigger to fully work through the governance process and prepare a SEEP, before moving onto the execution process.
- The scenario that leads to a solvent exit should form the basis of the financial modelling and be used to demonstrate how the metrics and triggers would work in practice.
- Understanding the cost of solvent exit is essential in demonstrating that the exit can be truly solvent. The business should be able to demonstrate a robust methodology for identifying all relevant costs, the timeline for the solvent exit and for incorporating the estimated cost of the solvent exit.

Five things internal audit should do

1. **Solvent exit analysis**
Internal audit should consider performing a review of the SEA against regulatory requirements, noting SEA is due by October 2025.
2. **Solvent exit execution plan**
Functions could combine this with an assessment of a firm's readiness to produce a SEEP. A SEEP needs to be prepared if solvent exit becomes a "reasonable prospect." It is also possible that the request to prepare the SEEP will come directly from the PRA, potentially for submission within 30 days of the request.
3. **Trigger frameworks**
Reviews should also include consideration of the trigger frameworks, with areas of focus including, ensuring appropriate calibration of existing indicators, beyond the point of simply indicating entry into recovery, and to the point at which orderly solvent exit would be triggered; and that the calibration of the trigger to develop the SEEP should therefore be separate from, and much earlier than, the trigger point at which a decision on commencing solvent exit becomes necessary.
4. **Financial modelling**
Consideration should be given to providing assurance over the SEA financial forecasting/modelling capabilities relating to solvent exit, ensuring the firm is able to produce required financial forecasts to accompany the SEA showing cash flows as well as an evolution of the profit and loss, balance sheet, capital and liquidity levels and any customer assets over the entire period.
5. **Cost methodology**
Finally internal audit could consider a review of the methodology for identifying all relevant costs relating to solvent exit. Areas of focus may include: an assessment of the minimum sale value of assets or portfolios needed to enable a successful solvent exit; a breakdown of the firm's assets or portfolios into those it would need to sell, transfer, or hold to maturity; and a breakdown of the firm's assets or portfolios into those which could be sold in a secondary market. It should also consider any exceptional costs that would be faced during solvent exit, e.g. redundancy.

To discuss this topic further, please get in touch.

Alex Brown
Partner
albrown@deloitte.co.uk

Henry Basing
Director
hbasing@deloitte.co.uk

01

New regulation and emerging risk

Internal audit's role in skilled persons review and regulatory issue validation

The Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA) have intensified supervisory scrutiny over financial institutions' risk management and governance, leading to increased enforcement actions through supervisory examinations and skilled person reviews. There have been around **70*** such regulatory reviews in the last 12 months focussed on areas of financial crime, regulatory reporting, controls and risk frameworks placing firms under pressure to ramp up their remediation.

Internal audit is increasingly being called upon to provide ongoing independent assurance activities to assess the regulatory remediation effort, supported by risk-based validation activities. Internal audit functions, whether directly impacted by the enforcement actions or asked to validate the corrective actions, face challenges in establishing a robust approach due to the significant size, scale and subject matter experience required.

Five things you should know

- The regulators enforce robust implementation of current regulations through tools such as PRA letters, FCA letters or skilled persons reviews. These tools are used where a regulator has concerns relating to a firm that could: impact operational or financial resilience; result in customer harm or affect market integrity. A firm's response to these, if not properly conducted, can lead to heightened scrutiny restrictions and fines.
- In addition to skilled persons reviews, the regulators may also use other tools to seek an opinion on the risk and control framework of a firm or to ensure compliance with regulatory expectations, such as a "shadow" skilled persons reports, which are instructed by the firms before being requested by the regulator's or attestation from a senior Board member about the control effectiveness and standard of compliance across the business.
- UK Financial Services organisations were fined more than **£126**** million in the first six months of 2024. Common root causes for the fines include: failure to mitigate the risks inherent in outsourcing the processing of data to its parent; inappropriate governance, controls and risk management framework; financial crime issues including KYC/AML/Take on; and non-compliance of conduct of business rules and prudential requirements.
- Issues raised during a regulatory review can often be interpreted differently therefore, clarity in roles and responsibilities, collaboration between the three lines of defence and periodic communication with regulators is vital for a robust issue validation program. This allows for diverse insights, adds value to the process and ensures that regulatory expectations are met.
- Internal audit, as a function, may also be subject to a skilled persons review, where they would be required to draft a remediation programme and ensure it is completed within the targeted timelines.

*source:
1. https://www.bankofengland.co.uk/prudential-regulation/supervision
2. https://www.fca.org.uk/about/how-we-regulate/supervision/skilled-persons-reviews

**source
1. 2024 fines | FCA.
2. https://www.bankofengland.co.uk/news/2024/may/pra-fines-citygroup-global-markets-limited.
3. https://www.bankofengland.co.uk/news/2024/january/pra-fines-hsbc-for-failures-in-deposit-protection-identification-and-notification.

Five things internal audit should do

1. **Regulatory remediation programme governance and attestation**
   Internal audit should look to provide assurance on the current design of the organisation's regulatory remediation programme, including governance structure and roles and responsibilities. The incorporation of attestations from relevant stakeholders and the embeddedness of this process is critical and as such should be in scope of the review.
2. **Remediation programme timeline**
   Internal audit should also consider and form a view regarding the firm's regulatory remediation programme timeline to ensure it has been designed to address regulators' identified risks and allows for effective internal audit involvement and challenge.
3. **Communication with stakeholders**
   Transparent and effective lines of communication with key stakeholders (regulatory bodies, senior management, external auditors and the Board) as well as the other lines of defence will be critical to highlight any challenges and provide periodic reporting on the status of internal audit's programme of work to the governance forums.
4. **Resourcing strategy**
   Internal audit will need to carefully evaluate the resourcing requirements for the validation programme so that this can be balanced against business-as-usual audit delivery.

   Internal audit functions will also need to ensure that the teams have the necessary regulatory understanding and experience to effectively validate compliance issues.
5. **Assessing the impact on control environment**
   Internal audit teams should assess the root cause of such regulatory issues and consider its impact on the overall control environment, including in instances where the scope of the remediation programme undergo changes or the programme encounters delays.

To discuss this topic further, please get in touch.

Mahmood Zaman
Director
mazaman@deloitte.co.uk

Nikhil Kulkarni
Associate director
nkulkarni@deloitte.co.uk

01

New regulation and emerging risk

Basel 3.1

The Prudential Regulation Authority (PRA) is in the process of finalising Basel 3.1. These rule changes are designed to implement the Basel 3 reforms, published by the Basel Committee on Banking Supervision (BCBS) in 2017, to address weaknesses identified during the financial crisis in the UK.

The PRA published its proposals in Consultation Paper 16/22 (CP16/22) in November 2022, and the first half of its near-final policy in December 2023 (PS17/23), covering market risk, counterparty credit risk, credit valuation adjustment and operational risk. A second near-final policy publication is expected imminently – delayed from an initial date in Q2 2024 – which will cover credit risk, credit risk mitigation and the output floor.

The current implementation date in the UK is 1 July 2025 (delayed from 1 January 2025), with the impact of the deferred publication of final rules not yet confirmed.

From a global perspective there is naturally some divergence in approach, in the content of the final rules and in timing. In general, the EU and Asia are further advanced in their implementation. For example, the majority of the rules in Hong Kong and Singapore came into force in mid-2024. Implementation in the US, whilst scheduled for 1 July 2025, is being impacted by the political environment, and there is industry opposition to the jurisdictional discretion taken by the US which is expected to increase overall capital requirements.

Five things you should know

- **Near-final policy part one:** Firms can implement the required, near-final changes with a higher degree of certainty. In general, the PRA has been faithful to the original BCBS text.
- **Near-final policy part two:** Whilst the final rules and implementation date are uncertain, the majority of firms have mobilised their programmes, given the extent of changes required. Firms may be well advised to continue on this basis, retaining the ability to change their solution based on the PRA's near-final policy.
- **Regulatory complexity:** The revised rules are more complex (operationally and technically) than current UK Capital Requirement Regulation (CRR) requirements. The rules introduce multiple new judgement points which could significantly impact capital requirements and business practices.
- **Pillar two uncertainty:** Rule changes have largely focused on Pillar one. As a result, the PRA plans to conduct an off-cycle review of bank-specific Pillar two capital requirements ahead of the implementation of Basel 3.1, to address potential double counting of capital and to avoid banks holding more (or less) capital than is warranted to address the underlying risk.
- **Small Domestic Deposit Taker regime (SDDT):** In parallel to Basel 3.1, the PRA is proposing to introduce a simplified capital framework for firms that meet the Small Domestic Deposit Taker regime (SDDT) criteria. The introduction of this regime in the UK will allow proportionality in the regulatory regime for smaller UK banks, reducing operational complexity and costs.

Five things internal audit should do

1. **Overall readiness**
Internal audit functions could consider reviewing implementation plans for operating model, technology, outsourcing, calculations, horizon scanning and governance, alongside the timeliness of proposed implementation.

2. **Regulatory interpretations and supporting governance**
Internal audit functions could review the completeness and robustness of the firm's regulatory interpretations, to determine whether they are consistent with the published rulebook, properly documented and justified, and to determine whether appropriate review and governance processes were followed. This may be more complex for firms with an international presence that are obliged to adhere to multiple – and sometimes conflicting – regulatory expectations.

3. **Data availability and solution design**
The proposed rules result in a significant number of additional data points (e.g. origination valuation, number of mortgaged properties and the currency of the obligor's income). Internal audit could assess the completeness of data availability and validate the revised data flow from source system to calculation and reporting.

4. **Assessment of firm-wide understanding and education**
The reforms are likely to result in significant downstream implications (e.g. on the firm's policies and processes, implications for the firm's lending strategy and potential portfolio expansion/reduction, financial planning and data and systems). Internal audit could assess the effectiveness of this education and communication, to determine whether other impacted teams are sufficiently well informed and engaged.

5. **Interactions with other programmes/priorities**
Depending on the size of the firm in question, the Basel 3.1 reforms may relate closely to other regulatory priorities (e.g. the SDDT and ongoing IRB model repair). Internal audit functions could challenge the Basel 3.1 programme to ensure dependencies are managed effectively and the firm's overarching regulatory strategy is coherent and robust.

To discuss this topic further, please get in touch.

Sinead Rothwell
Partner
srothwell@deloitte.co.uk

Andrew Freeman
Partner
anfreeman@deloitte.co.uk

01

New regulation and emerging risk

Employment taxes: engagement of off-payroll workers ("IR35")

Tax matters are often absent from internal audit plans, however employment tax is an area worthy of consideration, in particular the engagement of off-payroll workers (OPW). This area has the potential to result in material financial errors, impact on projects and business workstreams relying on OPW, and can cause reputational harm, including with HM Revenue and Customs (HMRC).

The "off-payroll workers in the private sector" legislation ("IR35" rules) was introduced in April 2021 for large and medium sized businesses. This reform to the taxation of Personal Service Companies (PSCs) was implemented by HM Treasury and HMRC to collect an additional estimated £1 billion of taxes from entities using off-payroll workers.

Under the changes, responsibility for undertaking employment status assessments of contractors became the responsibility of the entity using the services of the worker, or the "end-user". For contractors who are found to be "deemed" employees for tax purposes by the assessment, the entity paying the PSC is responsible for accounting for PAYE/NIC through payroll.

Five things you should know

- An "off-payroll worker", sometimes referred to as a "contractor" or "contingent worker", is an individual paid for their services outside of the payroll. The IR35 rules apply to workers coming through PSCs, partnerships, or other intermediaries.
- The IR35 rules, and employment status "tests", are complex and contain many nuances and subjective areas. There is no statutory definition of an employee for tax purposes, and so the facts and circumstances must be carefully examined against constantly evolving case law. The same employment status tests also apply for sole traders (or "self-employed" individuals).
- There is significant scope for businesses to make errors on a large scale when determining the employment status of off-payroll workers they engage. For example, the HMRC recently reached a settlement of £87.9m with a government department after the legislation was changed for the public sector in 2017.
- Businesses often find it difficult to identify the potentially impacted population of off-payroll workers engaged by their business.
- Failure to meet these obligations can result in unexpected PAYE/NIC liabilities for the end user (even where these would ordinarily sit with another party in the contractual chain). Payments of £100k to a contractor may give rise to potential tax liabilities of over £50k (plus interest and penalties) if HMRC decide that they should be a deemed an employee for tax.

Five things internal audit should do

1. **Recent HMRC activity**
To understand the situation, internal audit should determine if the business has an open enquiry with HMRC in respect of off-payroll workers, and if yes, understand the current status.

   Similarly, if the business has received the off-payroll working questionnaire from HMRC, has HMRC responded to this with any further questions or comments? If the business has not received the questionnaire, then internal audit should suggest the business complete the questionnaire and assess the completeness and accuracy of responses.

2. **Assess scale of potential risk**
Internal audit should work with management to understand the potential scale of the risk, identifying all off-payroll working engagements (including those in supply chains). Internal audit should also be mindful of changes to this position in the future, for example due to planned transformation or outsourcing activities.

3. **Establishing and assessing policies and processes in place**
When undertaking an audit in this space, functions should consider the governance framework relating to off-payroll workers including: a clear policy which sets out roles and responsibilities surrounding the compliance of engaging off-payroll workers; how new off-payroll worker engagements are identified; and how employment status assessments should be performed, reviewed and evidenced.

   Many internal audit functions will not have the in-house skillset to perform this review and may wish to engage third party specialist support.

4. **Independent qualitative testing**
Internal audit should carry out independent qualitative testing of the above polices, processes, assessments of off-payroll workers and controls.

5. **Ongoing compliance**
Internal audit should consider the design and operating effectiveness of controls in place to support periodic and trigger-based reviews of employment status assessments, as well as the ongoing training provided to those performing and reviewing the assessments.

To discuss this topic further, please get in touch.

Michael Nicolaides
Partner
mnicolaides@deloitte.co.uk

Samantha Mannall
Associate director
smannall@deloitte.co.uk

Payments and financial crime

Fraud

Financial crime

Payments regulation

02

Payments and financial crime

The role of internal audit in the prevention and detection of fraud

Fraud is now the most common criminal offence in the UK (Reference 1) and organisations across all industries and sectors continue to suffer sustained financial and reputational losses. As a result, expectations to prevent, detect and deter fraud are increasing. With the new Failure to Prevent Fraud Offence (FTP) and the corresponding implementation guidance on the immediate horizon, it is important that organisations and their senior stakeholders are comfortable with, and oversee the implementation of, robust fraud prevention measures including the strengthening of an anti-fraud risk framework.

In an environment where fraud is an ever-increasing threat and fraudsters continue to evolve and advance their techniques, internal audit should be a leading force in supporting organisations to enhance their approach to fraud prevention and detection.

Four things you should know

- Financial Services organisations have historically focused their efforts on addressing fraud risks both against their own organisation and its customers. However, the incoming offence will place a greater emphasis on fraud risks that could benefit the organisation, necessitating a fresh perspective on fraud prevention.
- As a result of the incoming FTP guidance, organisations should undertake an assessment to identify the key fraud risks faced from a FTP fraud perspective and ensure this process is regularly refreshed to account for changes in business activities and underlying risks.
- To manage the risk posed by fraud effectively, organisations should implement a fraud risk management framework that encapsulates six key elements: governance and leadership; risk assessment; controls identification; monitoring and assurance; training and awareness; and policies and procedures.
- These topics need to be overlayed with consideration of appropriate technology, robust well documented processes, and suitably skilled and capable individuals.

Seven things internal audit should do

1. **Maturity of the fraud risk management framework**
The approach taken to provide assurance on fraud should reflect the maturity of the organisation. For less mature organisations, this should focus on a review against the six key areas set out above. For more mature organisations, where audits of the framework have already been undertaken, internal audit should focus on the more specific areas highlighted as higher risk through the organisation's risk assessment.
2. **Enterprise-wide fraud risk assessment**
Internal audit should review the adequacy of the enterprise-wide fraud risk assessment, including the approach taken and rigour behind identifying the key risks and aligning these to business activities.
3. **Controls identification and mapping**
Functions should also consider assessing the design and operating effectiveness of the controls in place to mitigate the FTP fraud risks deemed to be the most significant to the organisation.
4. **Monitoring and assurance**
Key anti-fraud controls need to be subject to regular design and operational effectiveness testing, coordinated across the lines of defence. Progress on the fraud risk framework and assurance results should be regularly reported to the Board/audit committee. Organisations who are further ahead in maturity will be able demonstrate the use of analytics to monitor, identify and follow up on fraud red flags.
5. **Training and awareness**
Regular organisation-wide anti-fraud training should be provided, including specific targeted training for higher risk positions and / or functions.
6. **Policies and procedures**
Documented fraud risk policies should be in place, outlining the definition of fraud and key roles and responsibilities, such as a procedure on how to conduct and maintain a fraud risk assessment.
7. **Governance and leadership**
A strong and consistent 'tone from the top' is required to emphasise the importance of fraud awareness and the fact that fraud will not be tolerated.

To discuss this topic further, please get in touch.

James Meadowcroft
Partner
jmeadowcroft@deloitte.co.uk

Andreas Kozis
Senior manager
ankozis@deloitte.co.uk

https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/fraud-and-economic-crime#:~:text=Fraud%20remains%20the%20most%20common,billions%20of%20pounds%20every%20year

02

Payments and financial crime

Financial crime

Financial crime, such as money laundering, sanctions and fraud continue to be a growing issue for the UK. Despite the regulated sector allocating significant resource on compliance activity (billions of pounds per year in the UK by the public and private sectors[1]), to ensure that their products and services are not abused by criminals, the results do not necessarily lead to outcomes in combatting financial crime with as little as 1% of illicit funds[2] recovered annually.

Whilst businesses often do enough to not face regulatory scrutiny, this is usually at a great expense operationally – through ever-expanding financial crime teams to implement systems and controls which are not, unfortunately, delivering the desired outcomes.

Five things you should know

- Evolving nature of financial crime - The risk of fraud and money laundering is increasing through, for example, the use of social media, artificial intelligence, and cryptocurrencies. Financial crime is becoming increasingly sophisticated and diverse and as such the systems utilised to tackle this need to evolve and adapt to ensure they remain resilient.
- Geopolitical risk – The money laundering risk arising from attempts to evade applicable financial sanctions and export controls, for example, those imposed in response to Russia's invasion of Ukraine, demonstrate the need for a globally coordinated response to fix systemic gaps, which enable sanctions circumvention. A structure that does not prevent illicit financial flows encourages and finances transnational criminal activity, and will ultimately be a system where the efficacy of sanctions regimes, however devised, will always be called into question[3].
- Regulatory change – Policy makers are acutely aware of the challenges around financial crime and are proactively shaping new laws and regulations (e.g. ECCTA 2023) to enable public and private sector stakeholders to innovate and build more effective approaches, for example, through the range of initiatives in the Economic Crime Plan 2.0. Additionally, in the EU, the establishment of the Anti-Money Laundering Authority and the additional powers afforded under Article 75, enable the exchange of information through partnership, particularly with higher risk customers.
- Public Private Partnership (PPP) – Governments and industry bodies globally have realised that a better information sharing Public Private Partnership (PPP) is needed nationally and internationally, to allow information and intelligence sharing mechanisms that are required for a proactive response to tackling financial crime.
- Data systems and integration – There is significant fragmentation in data systems employed by both the public and private sector, which makes it difficult for data to be robustly shared and integrated. Government and industry bodies are looking at novel data sharing mechanisms, which facilitate timely identification of financial crime and an adequate assessment of risk.

Five things internal audit should do

1. **Auditing beyond compliance**
Whilst it is necessary to audit for compliance with regulatory obligations, functions should ensure they are challenging the effectiveness of systems and controls for financial crime more broadly.

2. **Technology and data enhancement**
Internal audit should consider the adequacy of the tools and systems in place to comply with the business' policy and regulatory expectations. Investment in advanced data analytics, such as machine learning tools, can significantly improve detection capabilities and longer-term efficiencies.

3. **Ensure resources remain commensurate to risk**
Whilst businesses continue investing to remain compliant, this does not always translate to an appropriately resourced team of suitably skilled individuals. As part of a review in this area internal audit should assess the skills, capabilities and capacity of the team, and their ability to absorb inevitable threats from the evolving financial crime landscape, which are appropriate for the risks faced by the organisation.

4. **Forward looking**
Often businesses are in a perpetual cycle of remediation based on responding to guidance from regulators. Internal audit should look beyond day-to-day activities to consider how the firm is scanning for emerging threats and driving ongoing refinement to their approach.

5. **Sourcing appropriate expertise**
Internal audit should consider how to best engage with industry experts to stay abreast of emerging threats and corresponding controls. Where this knowledge is not present in-house, functions should identify appropriate ways to source this.

1 LexisNexis Study: True Cost of Financial Crime Compliance Study – Europe, The Middle East and Africa, Study Reveals Annual Cost of Financial Crime Compliance Totals $85 Billion in EMEA
2 https://www.deloitte.com/global/en/Industries/financial-services/perspectives/global-financial-crime-prevention-detection-and-mitigation.html
3 "IIF Staff Paper on the Design and Implementation of Financial Sanctions". The Institute of International Finance

To discuss this topic further, please get in touch.

Katie Jackson
Partner
kjackson@deloitte.co.uk

Mo Wahed
Assistant director
mwahed@deloitte.co.uk

02

Payments and financial crime

Payments regulation

In 2024, payments are set to be one of the top priorities on the New EU Innovation Agenda and the UK Innovation policy agenda. Policymakers in both the UK and EU are currently introducing new regulations to bolster consumer protection, choice, and resilience for consumers. This includes promoting instant open banking payments, tackling fraud, and reviewing the Payment Services Directive 2 (PSD2) / e-money regimes, and digital IDs. Implementation is expected from 2024 onwards.

Complying with this complex web of new regulatory requirements will have significant implications for Payment Service Providers (PSPs), likely to include a need for additional skilled staff and financial resources. This will challenge PSPs' capacity to invest in new business and technological capabilities.

Internal audit teams need to look at these developments both from a horizon scanning and compliance perspective, but also from a strategic viewpoint to understand how regulatory considerations and changes may provide opportunities for innovation and technical developments.

Five things you should know

- The UK government is expected to publish the Payments National Vision later in 2024. This will set out the UK government's priorities for the payments industry. Future regulatory activity in the UK will be expected to follow this vision.
- **The EU Payment Services Directive 3 (PSD3) / Payment Services Regulation 1 (PSR1)** is expected to be finalised in early 2025 and will impact UK businesses with operations in the EU. The Financial Conduct Authority (FCA) is also expected to release the results of its review into the Payment Services Regulations (PSRs) in the near future.
- In a significant development to tackle Account Push Payment (APP) fraud, **mandatory reimbursement for consumers** will now be required from October 2024 at up to £415,000 per claim. The claim will be split between sending and receiving institutions.
- **Confirmation of payee is due to expand** to cover 99% of all faster payments transactions from October 2024. This impacts several hundred firms.
- From a financial crime perspective, **EU digital ID** wallets will be mandated which are intended to aid Anti-Money Laundering (AML) compliance while offering cost-effective and user-friendly identity verification across channels, potentially opening new revenue streams beyond financial services. Additionally, the use of artificial intelligence (AI) continues to be explored to help improve fraud detection and enhance the customer experience, meeting both supervisory and customer expectations.

Five things internal audit should do

1. **Understanding payments regulatory changes**
Internal audit may wish to consider performing a review of how the first and second line of defence is anticipating and responding to the numerous regulatory changes in payments, including horizon scanning processes to ensure that requirements will be assessed for impacts and compliance.

2. **Core payment regulation review**
Functions should assess how PSD3/PSR1 and the UK PSRs changes will impact their organisations, as well as existing and new product development processes. An assessment of how new requirements will be dealt with from a compliance perspective is also encouraged.

3. **Innovation impact assessment**
Functions should look to gain an understanding of what activities are being undertaken to drive innovation as a result of new regulatory changes relevant to their business.

4. **Review of fraud developments**
Internal audit should explore how cost implications of the APP fraud reimbursement model are being dealt with and how/whether AI solutions are being utilised to help reduce payment fraud.

5. **Project delivery assessment**
Internal audit should consider providing real time feedback and assurance over projects in place to deliver change programmes in response to regulatory developments.

To discuss this topic further, please get in touch.

Steven Bailey
Director
sjbailey@deloitte.co.uk

Sukhjit Saundh
Associate director
sssaundh@deloitte.co.uk

Prudential and credit risk

Liquidity risk management

Credit risk

Model risk management

03

Prudential and credit risk

Liquidity risk management

Regulators and supervisors have raised the priority of liquidity and funding risks since the banking market stresses in March 2023. Local and international policy setters have been looking at lessons that firms and supervisors should learn to improve the management of liquidity risks and ensure more effective supervision.

The Prudential Regulatory Authority (PRA) and European Central Bank (ECB) have signalled increased scrutiny of how firms manage liquidity and the effect of normalisation of monetary policy on firms' funding plans over the next few years. A recent multi-firm review by the Financial Conduct Authority (FCA) of investment and asset managers found significant deficiencies in firms' understanding of methodologies used in liquidity stress testing.

Five things you should know

- Improvements in stress testing assumptions and capabilities, especially in terms of concentration of deposits and effectiveness, testability and diversification of contingency funding plans has already been the focus of recent supervisory activity.
- The ECB recently increased the frequency of liquidity reporting demands, and we expect other supervisors to follow, in terms of frequency and quality of liquidity submissions.
- There is significant cross-industry focus on the liquidity risks stemming from heightened market volatility and associated margin requirements. Events such as the 2022 UK "Mini Budget" and the Ukraine/Russia war have exposed shortcomings in liquidity risk management following market-driven stresses. The FCA in particular has placed significant focus on this topic over the past year for investment firms. The Financial Stability Board (FSB) has consulted on non-bank financial institutions (NBFI)'s liquidity preparedness for margin calls, recommending the establishment of liquidity risk appetite for margin calls and to conduct liquidity stress testing covering a range of extreme but plausible scenarios.
- The PRA recently highlighted the need for counterparties to stay prepared for potential liquidity requirements arising from sharp margin calls in a stress to reduce procyclical behaviours. This requires getting margin and haircut levels right, which in turn entails a higher degree of transparency, effective stress testing, and improvements to operational processes.
- In a recent supervisory newsletter, the ECB expressed concerns over how some internal audit functions provide oversight of liquidity citing: (i) limited involvement of the management body in overseeing the effectiveness of internal audit functions; (ii) non-comprehensive audit plans on the implementation of risk-appetite framework, C&E and liquidity risks; (iii) inadequate audit staffing, especially around IT and cybersecurity expertise.

Five things internal audit should do

1. **Regulatory reporting (Banks)**
The PRA expects banks to improve their controls over upstream data lineage, end-to-end process and controls documentation that feeds into the liquidity reporting stream. As such internal audit should consider focussing work on these areas.

2. **Internal Liquidity Adequacy Assessment Process (ILAAP) (Banks)**
Internal auditors are expected to confidently talk supervisors through the methodologies used to identify, manage, and control liquidity risks, especially those related to deposit flights, instability of deposits and concentration of funds. Some functions will need to consider access to specialists or training to facilitate this.

3. **Internal Capital and Risk Assessment (ICARA) process (Investment firms)**
Supervisors will look at whether investment firms' internal audit is adequately using the ICARA process to improve the understanding of liquidity positioning, preparedness on margin calls, and controls on intra-day liquidity availability.

   Internal audit should focus on controls over the quantification of firms' liquid assets, the breakdown of inflows and outflows in wind-down scenarios, and over the availability of releasable assets in contingency funding contexts.

4. **Regulatory liquidity feedback (Banks and investment firms)**
The FCA gave several wholesale brokers material feedback on liquidity risk management. Banks have received detailed liquidity feedback arising from Liquidity Supervisory Review and Evaluation Process (L-SREP) reviews.

   Firms' internal audit functions should improve the escalation process for supervisors' findings and feedback, setting clear remediation actions and related timings.

5. **Insurers**
Insurers in scope of upcoming reporting rules – to be published for consultation by the PRA by Q1 2025 – may need to upgrade the granularity and update the frequency of their liquidity risk metrics, which will require internal audit to review. Insurers may also engage internal audit in reviewing potential liquidity risk exposures as a part of their life insurance stress test work.

To discuss this topic further, please get in touch.

Rod Hardcastle
Director
rhardcastle@deloitte.co.uk

Luca Pagani
Senior consultant
lpagani@deloitte.co.uk

03

Prudential and credit risk

Credit risk

Since the end of 2019 the UK economy has been through a turbulent time. From a credit risk point of view most UK households and corporates have been resilient, although many borrowers continue to face pressures and credit officers are cautious given the risk from lagged defaults and "hot spots" of higher risk lending. As the economy enters a new phase it is crucial to maintain robust governance, controls, and reporting for credit risk, ensuring that models remain suitable and perform as expected, especially in the context of ongoing economic and geopolitical uncertainties.

Four things you should know

- **Modelling design, assumptions, and limitations:** The credit landscape continues to evolve and is significantly different from the pre-COVID era. This poses challenges for model calibration, especially given benign credit performance alongside significant economic volatility since the start of 2020. As a result, there's the risk that some of the intricate quantitative assumptions and expert judgements, critical for provision and capital modelling, may be unsuitable in the absence of data-based calibration. The model design and assumptions need to be reviewed and overlays might need to be introduced to mitigate these risks.
- **Management judgments and overlays:** Higher mortgage rates continue to put pressure on household finances and highly leveraged corporates face significant refinancing challenges. These factors aren't always captured within the model output and require the use of overlays and management judgments to reflect the credit risk faced by different households, businesses, and sectors. However, these overlays and judgements are frequently applied on a broad portfolio level based on highly approximate approaches. There is a risk that these judgments might fall short of adequately mitigating the risk for vulnerable customers and sectors. As highlighted in the European Central Bank's (ECB) latest report on overlays and novel risks[1] , regulators continue to encourage firms to transition towards more granular, account-level overlays.
- **Credit risk governance:** Credit risk governance is critical in ensuring the safety and soundness of financial institutions, especially during uncertain times. Effective governance includes the timely identification and management of vulnerable sectors, setting of appropriate risk appetite strategies, validating complex models together with monitoring the above. Governance frameworks often lack a forward-looking approach and could fail to capture emerging risks. Given the unique macro-landscape, it will be important to assess whether the credit risk governance frameworks remain suitable and capable of addressing potential risk "hot spots".
- **Data and reporting:** The ability of a firm's management to identify, quantify and mitigate risk is critically dependent on data and reporting. Reporting frameworks often struggle to capture and communicate key and emerging risks and fail to use the broad sources of data available consistently and effectively. Data quality controls including data lineage and data dictionaries are critical for ensuring quality and traceability of the data across process.

1 IFRS 9 overlays and model improvements for novel risks (europa.eu)

Four things internal audit should do

1. **Modelling design, assumptions, and limitations**
Internal audit should assess whether the models have been sufficiently reviewed and challenged regarding their design suitability and underlying assumptions in response to the changing macroeconomic landscape. The review should consider the model's assumptions/limitations and evaluate whether adequate mitigation measures have been implemented. This can include further evaluation of the design and effectiveness of model risk controls to manage model risk.
2. **Management judgements and overlays**
A targeted review could be considered to evaluate the framework and identify where management judgment is required, as well as assess the completeness and suitability of model overlays introduced. This can include a specific focus on the impact of high interest rates on households and businesses. The review should scrutinise the adequacy of oversight of the judgements made, and focus on the quality and detail of the documentation of judgements/ assumptions to ensure their consistent application.
3. **Credit risk governance**
Functions should consider assessing the design and effectiveness of the credit risk management framework in identifying and tracking key and emerging risks. This could include reviewing credit risk policies, risk appetite, and processes in place to monitor and validate models. Internal audit could also consider assessing the robustness of governance frameworks including the review of the structure, accountabilities, and responsibilities of committees.
4. **Data and reporting**
Internal audit could consider assessing the sufficiency and appropriateness of the reporting structure and management information, with a focus on primary metrics reported to committees and how the MI supports effective decision making. The review should also assess the design and effectiveness of data quality controls.

To discuss this topic further, please get in touch.

Richard Tedder
Partner
rtedder@deloitte.co.uk

Tim Alberts
Director
talberts@deloitte.co.uk

03

Prudential and credit risk

Model risk management

The model risk management principles for banks supervisory statement (SS1/23), originally published in May 2023, came into effect on 17 May 2024. Whilst the statement applies to banks with existing permissions to use internal models for capital purposes, the scope of the supervisory statement is likely to widen and other banks, insurers and asset managers should also consider the proposals to manage model risk.

The Prudential Regulation Authority (PRA) has proposed five principles as the core disciplines for a sound framework to effectively manage model risk, along with a very broad definition of what constitutes a model for the purposes of the principles.

Five things you should know

- The model risk management supervisory statement SS1/23 is now live; however, many banks are experiencing challenges fundamentally changing how they handle model risk. At its heart, SS1/23 is intended to influence culture and banks needs to demonstrate an improving model culture.
- The PRA's principles for model risk management (MRM) place considerable expectations on the role of board members with stronger governance oversight coming through increased involvement of board and senior management, setting of model risk appetite, approval of MRM policy and appointment of senior management function (SMF) to be accountable for the overall MRM framework.
- The MRM principles present higher than expected challenges, including the need for an expanded definition of models to include deterministic quantitative methods (DQMs) which for many banks has significantly increased the number of items classified as models, more complex tiering requirements and increased level of detail in the model inventory.
- The principles allow banks to interpret them based on their size and complexity, however less regulatory prescription inevitably means reduced clarity on what will constitute a compliant approach.
- SS1/23 mandates firms to complete an annual self-assessment against the principles and, prepare remediation plans as needed. The PRA has asked several banks to submit their SS1/23 gap analysis and remediation plans. Banks not requested by the PRA to submit their plans can expect model risk on the agenda for upcoming supervisory meetings.

Five things internal audit should do

1. **Assess the model risk management framework**
Internal audit should first look to understand the major changes introduced through the SS1/23 requirements, including the broadened model definition, model tiering, model risk appetite, and the appointing of an accountable senior manager (SMF). This positions the function well to consider how best to integrate these topics into the audit plan.

2. **Review policies and procedures**
A starting position for many functions will be to assess whether policies and procedures have been adequately revised to align with SS1/23. Also, whether they are well understood and are followed throughout the firm across all three lines of defence, in relation to all model types (including AI/ML and GenAI applications).

3. **Model validation processes and skills gap**
Internal audit should consider assessing the validation activities of the firm including; the risk controls and validation activities and the adequacy of these for the level of model risk / tiering; the validation of teams' capacity and skills to provide adequate challenge to a wider scope of models, report limitations and escalate material findings.

4. **Monitor compliance and reporting**
Internal audit should ensure their audit universe includes a periodic assessment of the effectiveness of the MRM framework and adherence to policies, which may involve a detailed review of self-assessments and ongoing remediation plans for any deficiencies.

5. **Other banks, insurers and asset managers**
Regulation of model risk is expected to follow shortly in other areas. As such, functions for these firms should undertake an audit to understand the baseline of the MRM framework, and the firms preparedness for enhancements in the overall maturity of its approach to models.

To discuss this topic further, please get in touch.

Richard Tedder
Partner
rtedder@deloitte.co.uk

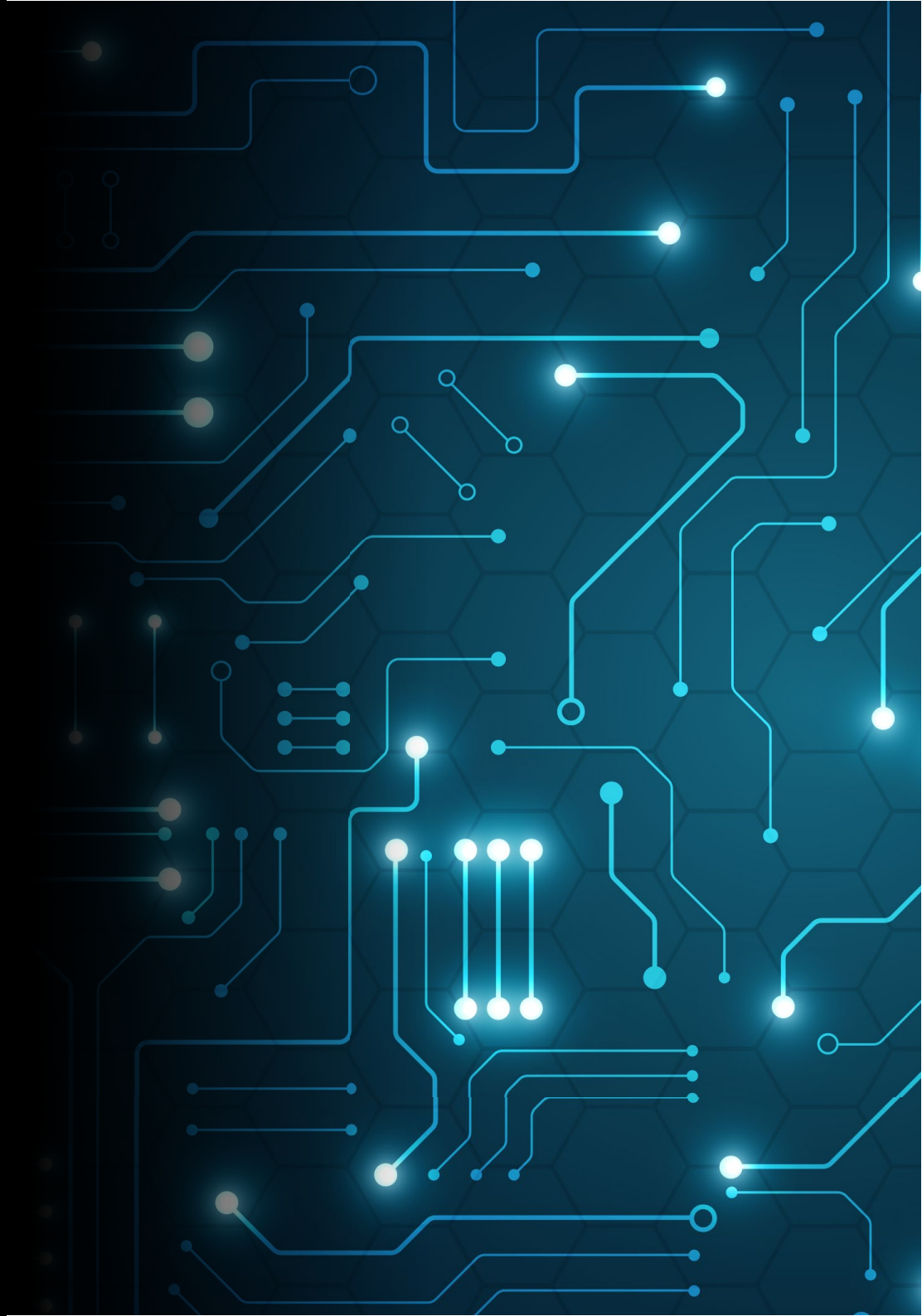
Jyoti Makolski
Associate director
jmakolski@deloitte.co.uk

Governance

UK Corporate Governance Code

Risk culture

Third party risk management



04

Governance

UK Corporate Governance Code

The Financial Reporting Council (FRC) issued a revised UK Corporate Governance Code (the Code) on 22 January 2024, emphasising a principles-based approach to strengthen board oversight of internal controls. There are key changes that impact how internal audit can support their organisations in navigating this evolving landscape.

The 2024 Code applies to accounting periods beginning on or after 1 January 2025, with the exception of Provision 29, which requires an annual Board declaration on the effectiveness of material internal controls at the balance sheet date. This provision is applicable for accounting periods beginning on or after 1 January 2026 and captures financial, reporting, operational and compliance controls that are deemed to be material by the Board.

It is proposed that the Board provides the following disclosure in the annual report:

- a description of how the board has monitored and reviewed the effectiveness of the risk management and internal control framework;
- a declaration of effectiveness of the material controls at the balance sheet date; and
- a description of any material controls which have not operated effectively at the balance sheet date, the action taken, or proposed, to improve them and any action taken to address previously reported issues.

Five things you should know

- Board leadership and company purpose: The UK Corporate Governance Code places a strong emphasis on the role of the board of directors in providing effective leadership and oversight to promote the long-term sustainable success of the company, generating value for shareholders, and contributing to wider society.
- Division of responsibilities: This section of the Code highlights the importance of the diverse board composition, independent directors, and the establishment of clear responsibilities between the leadership of the board and executive leadership of the company's business.
- Composition, succession and evaluation: The Code emphasises the formal, rigorous, and transparent procedure, and an effective succession plan for the board and senior management to ensure that diversity, inclusion, and equal opportunity is promoted. It further emphasises the need to establish a nomination committee to lead the process for appointments and ensure succession plans are in place.
- Audit, risk, and internal control: The Code emphasises the need for companies to establish robust risk management processes, an internal control framework and to determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives.
- Remuneration: The code addresses the issue of executive remuneration, advocating for a remuneration structure that aligns with the long-term interests of the company and its shareholders. It also promotes accountability by requiring companies to disclose clear and comprehensive information regarding executive pay.

The updated Code is supported by newly issued guidance, the 2024 Code Guidance, which aims to bring together the most relevant content from previous publications into a single, condensed, digitally accessible and user-friendly resource. The FRC is keen to reiterate that the guidance is not part of the Code, but a separate collection of information designed to help the application of the Code to different companies' needs.

Five things internal audit should do

1. **Code readiness assessment**
   Evaluate the organisation's current state against the new Code, identify gaps, and recommend enhancements to governance processes.
2. **Implementation project assurance**
   Provide assurance on the implementation of the Code, including reviewing project governance, risk management processes, and the design and effectiveness of controls.
3. **Internal control maturity assessment**
   Benchmark the maturity of the organisation's internal control framework against industry best practices and identify areas for improvement.
4. **Assurance mapping**
   Develop a comprehensive assurance map to identify gaps and overlaps in assurance coverage across the organisation, supporting the board's declaration on internal control effectiveness.
5. **Ongoing assurance on the control environment**
   Provide ongoing assurance to the board on the effectiveness of material controls, aligning internal audit plans to support this activity and securing necessary resources.

To discuss this topic further, please get in touch.

Louis MacMillan
Partner
lmacmillan@deloitte.co.uk

Saroj Mandhwani
Manager
smandhwani@deloitte.co.uk

To discuss this topic further, please get in touch.

Jessica Sutherland
Director
jessicasutherland@deloitte.co.uk

04

Governance

Risk culture

Organisations with a strong desirable culture overall, and risk culture more specifically, outperform those with undesirable cultures[1]. They tend to be more trustworthy and appealing to customers and employees alike and are better placed to achieve long-term sustainability. Setting or transforming a business culture should be an active and conscious process incorporating design thinking, agile executions, culture enablement coaches, and other culture tools and accelerators.

Five things you should know

- In Financial Services, UK regulators are increasing their culture supervision and expectations. An organisation's Chairman must have responsibility for overseeing day-to-day firm culture and take responsibility for leading the development of the culture. From a Consumer Duty perspective, there are also inherent links to risk culture. For example, firms must appoint a Consumer Duty champion and the Financial Conduct Authority (FCA) expects annual assessments of culture and alignment to the Duty.
- A risk intelligent and purpose-led culture (i.e. one that has values at the forefront and is consistently driven by these) is not only a regulatory priority, but it has business benefits and it is critical for supporting good customer outcomes. A risk intelligent culture means that everyone understands the organisation's approach to risk, takes personal responsibility to manage risk in everything they do, and encourages others to follow their example.
- Best practice is for an organisation to define a compelling cultural aspiration which is aligned to its mission, vision, values, and strategy.
- Before a business can seek to change its culture, it will need to appropriately assess the culture to understand the existing behaviours and mindsets and, the shifts needed to achieve transformational culture change. There are several ways firms can assess their risk cultures, through diagnostic surveys, focus groups, interviews, leadership labs and risk culture gap analysis.
- Risk culture measurement metrics enable Boards and executive teams to gain a better understanding of their organisation's risk culture to make informed decisions on cultural matters. Defining an appropriate set of risk culture metrics will be an iterative process that firms should be thinking about starting now.

Five things internal audit should do

1. **Risk culture assessment**
Consider an organisation-wide risk culture infrastructure review and risk culture diagnostic survey, including industry benchmarking. This could also be considered as part of audits looking at dimensions such as embeddedness of the Duty, governance or Board effectiveness.

2. **Tone at the top**
Evaluating the influence of senior management and the board on shaping the risk culture and demonstration of ethical decision-making is another area internal audit could consider. The influence of middle management should also be included in scope. This can be evaluated via surveys or deeper-dive activities such as focus groups or interviews.

3. **Risk culture governance**
Functions may want to include a review focussing on the effectiveness of the risk governance framework in promoting a strong risk culture.

4. **Employee training and awareness**
Internal audit should consider assessing the adequacy of training programmes and communication strategies aimed at enhancing risk awareness.

5. **Risk reporting**
Internal audit can consider a review of the metrics suite that covers key dimensions of the organisation's population demographics, and which will be able to track trends over time. The range of metrics, balancing qualitative and quantitative, how they have been defined and reporting accuracy would be important scope elements.

1 London Research Network, Benchmark of Ethical Culture, https://pages.lrn.com/hubfs/Benchmark_of_Ethical_Culture_LRN.pdf

04

Governance

Third party risk management (TPRM)

Management of third-party risk continues to face significant scrutiny, recognising in particular the crucial role third parties play in providing important business services (IBS). There are known challenges in handling supply chains, managing visibility of extended third-party relationships, and navigating geopolitical and macro-economic landscape.

Many organisations will have experienced disruption of business services supported by critical third-parties due to issues such as cyber-attacks, data breaches and compliance failures. Our Global TPRM survey has shown that mature TPRM practices are based on deeper trust and transparency with third parties.

Five things you should know

- The EU and UK authorities are set to finalise their proposed approach[1] for overseeing critical third parties by early 2025. Third parties that expect to be designated as critical in both the UK and the EU can start evaluating an optimal and coordinated approach to implementation.
- As the Prudential Regulation Authority (PRA) and EU's **operational resilience requirements** transition deadline approaches in Q1 2025, organisations must strengthen the connection between operational resilience and existing third-party frameworks to ensure impact tolerance limits are not impacted by disruption at third parties.
- **Prescriptive regulatory requirements** and increased third-party disruptions have intensified regulatory scrutiny, prompting large-scale remediation and transformation activities that require greater collaboration across all three lines of defence.
- An organisation's use **of new technologies** to manage third-party risk, including using Generative AI (GenAI) based tools, should prompt a review of the TPRM framework to evaluate emerging AI related risks (e.g. underlying data quality, algorithm reliability, cybersecurity, data privacy, and ethical considerations), as these may give rise to reputational and financial risks.
- The Corporate Sustainability Reporting Directive (CSRD) requires firms to define and report on sustainability impacts, risks and opportunities across both direct and indirect business relationships within their upstream and downstream value chains. TPRM frameworks must adapt to incorporate **critical ESG considerations;** recognising an increasing need to evaluate and report on sustainability risks beyond the organisation's own activities.

Five things internal audit should do

1. **Integration and embeddedness of regulatory requirements**
   Internal audit should consider undertaking a review to assess the embeddedness of regulatory requirements.
   As well as testing integration of the regulatory requirements the review could consider: the adequacy of compliance reporting to management and the Board; third-party contract compliance with regulations; record-keeping; monitoring intra-group arrangements; efficacy of third-party risk assessment; and monitoring to mitigate service disrupting risks.
2. **Integrated approach to third-party management**
   A common root-cause of ineffective TPRM stems from the absence of a cross functional and enterprise-wide framework.
   Internal audit should challenge the TPRM operating model and its integration with relevant functions to understand how silos are avoided and synergies realised. The approach here should also look at the clarity of roles and responsibilities to ensure a comprehensive risk monitoring, and consistent third-party record-keeping .
3. **Resilience across the supply chain**
   Audits looking at operational resilience should include adequate coverage of third parties. Internal audit should evaluate how third-party roles are linked to the firm's operational resilience requirements and assess how the impact of third parties on IBS has been evaluated, as well as the calibration of tolerance limits. The review could also consider how third-party failures have been incorporated in stress testing scenarios and the adequacy of BCP and exit plans for critical third parties.
4. **Concentration risk across extended supply chain**
   Internal audit should look to understand how its business has ensured that appropriate metrics are in place to detect concentration risks that may exist within the supply chain, across multiple dimensions. The adequacy of mitigation actions to minimise concentration, and the processes to swiftly substitute third parties should also be considered.
5. **Emerging risks**
   Internal audit may wish to consider assessing the maturity of the TPRM framework to address emerging risks, including AI-related risks from third-party use and TPRM impacts and opportunities in relation to CSRD reporting.

[1] Critical third parties (CTPs) – navigating the EU's and UK's new regulatory frameworks | Deloitte UK

To discuss this topic further, please get in touch.

Talal Sangar Raja
Senior manager
traja@deloitte.co.uk

Disha Thakkar
Senior manager
dishathakkar@deloitte.co.uk

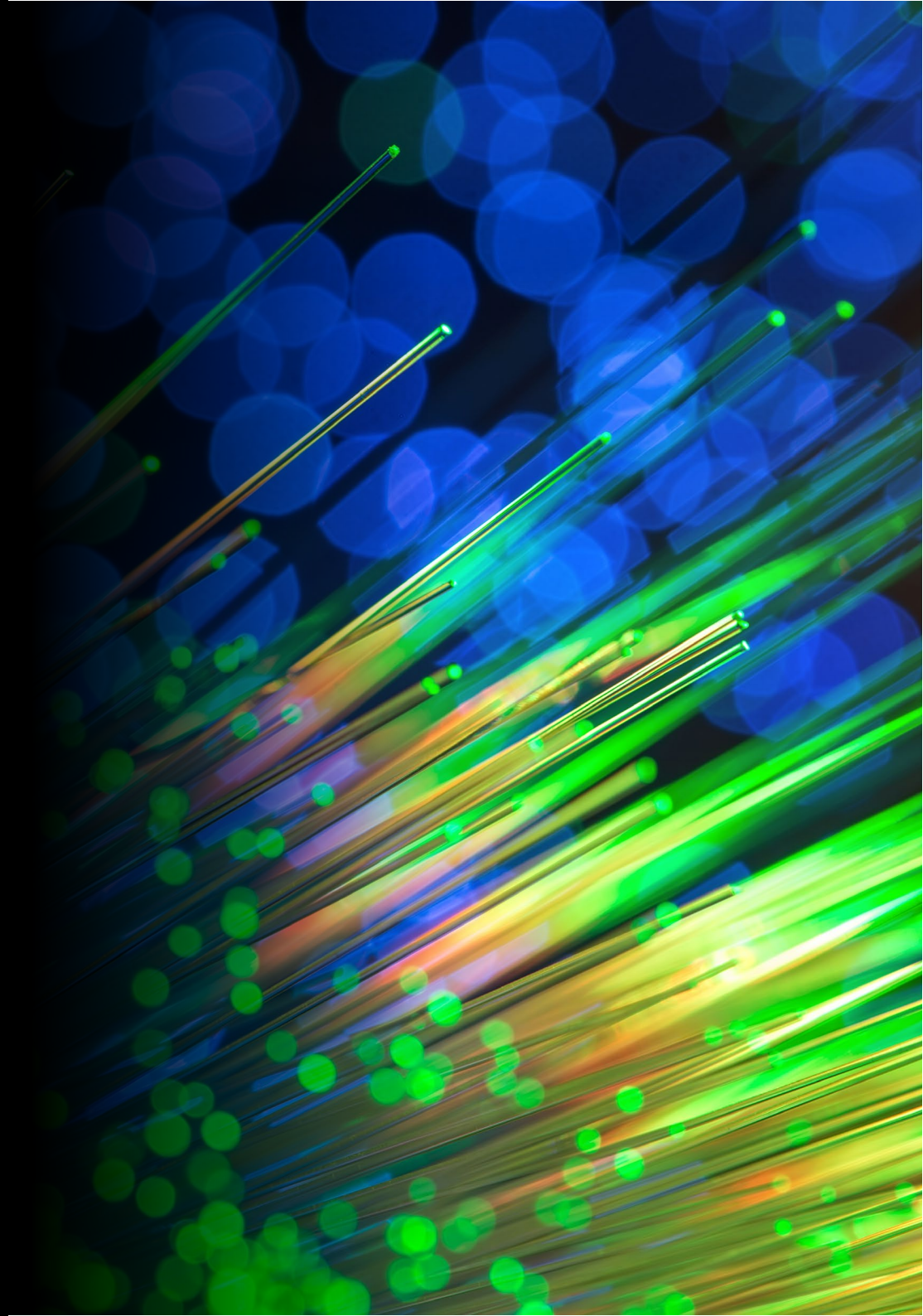
ESG

Sustainability disclosures

Transition planning and transition finance

Diversity and inclusion

Non-financial misconduct



05

ESG

Sustainability reporting and disclosures

The last 18 months have seen pivotal shifts in the landscape for sustainability reporting, at a UK, European and global level. Key reporting requirements – including the Corporate Sustainability Reporting Directive (CSRD) and the International Sustainable Standards Board (ISSB) – are now known, but the standards themselves continue to develop. The overall trend is towards enhanced transparency about, and accountability for, critical sustainability practices, topics and behaviours. Forward looking firms will take no-regret actions now to prepare for incoming regulation and will develop integrated reporting processes that span the multiple requirements.

Four things you should know

- The Financial Conduct Authority (FCA) has now published its final rules and guidance on Sustainability Disclosure Requirements (UK SDR) and investment labels. These impact UK firms that manage investment funds and FCA-authorised firms (domiciled in the UK) that make sustainability claims in their marketing about their products and services (anti-greenwashing rule).
- For qualifying firms, CSRD reporting requirements are now effective with first reporting due from 2025. 2023 saw the ISSB release IFRS S1 and S2 – disclosure requirements for companies to inform investors about the sustainability-related risks and opportunities they face over the short, medium, and long term. In the UK, these are expected to be endorsed in Q4 2024 / Q1 2025 and adopted through the Sustainable Disclosure Standard framework.
- In September 2023, the taskforce on Nature-related Financial Disclosures (TNFD) published its final recommendations for nature-related risk management and disclosures. The European Financial Reporting Advisory Group and ISSB are expected to clarify how the final TNFD framework on nature-related disclosures will be adopted. Over 300 companies have already signalled early adoption and have committed to disclose in accordance with TNFD recommendations by 2025 or earlier.
- Mandatory disclosures on diversity and inclusion (D&I) are on the horizon following Prudential Regulation Authority (PRA) and FCA consultations on this topic in 2023. In the financial sector, this would include D&I monitoring, regulatory reporting and public disclosures.

Five things internal audit should do

1. **Anti-greenwashing rule**
The new rule will require firms to assess their marketing materials, call scripts and other sales materials to ensure compliance. Internal audit can support this vital work by ensuring there are appropriate detective controls in place to identify non-compliant marketing; and preventative controls to ensure that greenwashing is mitigated during the product development phase.

2. **Internal audit strategy and position**
Internal audit must apply a strategic and long-term lens in developing an audit plan, which can provide iterative and ongoing assurance in line with the evolving risks. A co-ordinated approach with other lines of defence will be critical to ensure suitable coverage across the growing number of reporting requirements.

3. **Reasonable assurance**
CSRD will require that firms obtain reasonable assurance in the coming years across their related disclosures. Internal audit must position themselves as a strategic business partner within the organisation in helping build and test the resilience of the underlying control framework.

4. **New data and processes**
Many of the new ESG reporting data points, together with the data collection processes, will be new for most firms. Internal audit should urgently identify the firm's data governance maturity and ensure third line efforts are prioritised accordingly.

5. **Business opportunity and integration**
Inherently, internal auditors are focussed on the risks facing an organisation. However, third line should consider how to support and advise on the related opportunities through ESG related reporting, in the context of market positioning and sustainability strategy. Internal audit must also capitalise on its holistic view and recommend ways to link and streamline reporting processes. This will reduce reporting silos, increase efficiency and drive effective integration across the ESG reporting framework.

To discuss this topic further, please get in touch.

Hetty van der Wal
Associate director
hevanderwal@deloitte.co.uk

Sarah Cook
Senior manager
sacook@deloitte.co.uk

05

ESG

Transition planning, transition finance

Regulatory and consumer scrutiny around potential 'greenwashing' and 'greenhushing' is at an all-time high. Developing a robust climate transition plan is becoming even more critical for organisations, as they look to set out plans to deliver on climate targets and build trust with external stakeholders.

In recent months we have seen a sharp increase in the number and nature of entities required to develop and disclose their forward-looking transition plans, and we anticipate this trend will continue as regulators look to align the industry with UK government net-zero goals. Increasingly, there is also a call for the integration of climate transition plans with financial reporting.

A core component of transition planning is the development of financial products and services that support long-term decarbonisation, referred to as 'transition finance'. Recognising the significant industry opportunity, in January 2024 saw the UK government launch a transition finance market review to identify how the UK finance and professional services sectors can become global transition finance leaders.

Five things you should know

- Entities in scope for the Corporate Sustainability Reporting Directive (CSRD) must disclose transition plans and explain how their targets are compatible with limiting global warming to 1.5 degrees Celsius.
- Per incoming Financial Conduct Authority (FCA) rules, it will become mandatory for UK-listed issuers to make transition plan disclosures for accounting periods after January 2025.
- For companies that have already developed a transition plan, ISSB IFRS S2 (applicable for accounting periods from January 2024) requires disclosure of critical assumptions and/or dependencies of the transition plan as well as plans around how transition activities will be resourced.
- To help companies create and disclose effective transition plans in the United Kingdom, the UK Government launched the transition plan taskforce (TPT) to develop a gold standard framework and in April 2024 released its final set of sector-specific guidance. The application of the TPT disclosure framework is currently voluntary, however this is expected to change as the FCA looks to align disclosure requirements with the TPT framework and ISSB Standards.
- Firms offering transition finance products have been subject to the FCA's Sustainability Disclosure Requirements and investment regime for UK-based funds as of November 2023. The rules cover all FCA-authorised firms and include an anti-greenwashing rule effective from 31 May 2024, with remaining requirements to be passed in over the period to December 2026.

Five things internal audit should do

1. **Engagement and governance**
Internal audit should challenge whether there is sufficient engagement across the organisation to deliver the required organisation-wide changes. A review in this area should include considerations of governance frameworks and clarity of roles and responsibilities and how these have been embedded to drive accountability.

2. **Capacity and skills**
As with many ESG related topics, transition planning is a complex, technical, and wide-reaching area and many organisations are struggling to find appropriately skilled and experienced individuals to design and implement related activities. Internal audit must challenge whether the business is adequately resourced to drive effective change.

3. **Data**
Internal audit should consider performing an audit in the area of ESG related data which is an area many businesses are currently struggling with. This should include an assessment of the resilience of data infrastructure and quality and reliability of the data underpinning the transition plan.

4. **Assumptions**
In order to drive the transition plan resiliency, internal audit should independently evaluate the validity of assumptions and dependencies, help identify the related sensitivities and ensure follow on actions are embedded.

5. **Transition finance**
Internal audit should assess how the business is responding to emerging disclosure requirements and interactions with other reporting rules. Internal audit should also ensure there is sufficient flexibility, capacity and skills within the organisation to implement required changes.

To discuss this topic further, please get in touch.

Hetty van der Wal
Associate director
hevanderwal@deloitte.co.uk

Sarah Cook
Senior manager
sacook@deloitte.co.uk

05

ESG

Diversity and inclusion

Recently there has been a shift in focus regarding how organisations approach diversity and inclusion (D&I) within their business. Whilst D&I policies and frameworks have always existed, in recent months, the industry regulators have raised the expectations for financial services' firms. Late 2023 saw the Financial Conduct Authority (FCA) and the Prudential Regulation Authority (PRA) publish consultations setting out their proposals to introduce a new regulatory framework on D&I in the financial sector. The proposals reference the fundamental link between D&I and culture, and firms must treat D&I as a cultural issue and opportunity. The proposals also included a new framework for managing non-financial misconduct (NFM) stating that NFM reduces psychological safety and inhibits the "speaking up" of employees. Please see the separate article in this report on NFM.

Five things you should know

- The proposals focus on firms' reporting of D&I data to the regulators and making D&I disclosures to the public. This data will include but is not limited to, information around age, sexual orientation, gender, disability, ethnicity, religion, parental and carer responsibilities, and socio-economic background.
- Firms will need to establish, implement, and maintain an effective D&I strategy that covers a number of minimum requirements and should be overseen by the Board, under the proposed rules.
- Disclosing periodically against set diversity targets in line with their D&I strategy would also be required, encouraging accountability and ensuring that progress can be effectively monitored.
- Critically the proposal sets out plans to better integrate NFM considerations into staff fitness and propriety assessments, conduct rules and the suitability criteria for firms to operate in the financial sector.
- A recent speech by the FCA CEO indicated a significant number of responses has meant progressing with the NFM elements of the proposal will be prioritised for 2024; and further consideration on the proposed D&I rules is needed before rules in this area can be progressed.

Five things internal audit should do

1. **D&I strategy**
   Internal audit can support the development of the D&I strategy through assessment against the PRA expectations, and to challenge the alignment of the firms D&I strategy against the organisations broader mission, existing frameworks, and employee engagement. One example would be ensuring recruitment processes are aligned with strategic ambitions.
2. **D&I targets**
   The regulator expects firms to analyse evidence collected on the state of diversity and inclusion to help inform the targets set. Internal audit should challenge the suitability of these inputs and ensure there is clear linkage of defined targets to the strategic objectives, ensuring firms avoid setting tick-box targets.
3. **Data reporting and disclosure**
   Functions could also support organisations with an initial gap analysis to identify where existing gaps exist across data availability and reporting capabilities, whilst also assessing the resiliency of related remediation activities.
4. **Governance and risk management**
   The regulatory messaging states that D&I should be treated as a non-financial risk, and risk functions, together with internal audit, can play an important role in managing the risk. Internal audit should evaluate the embeddedness of D&I within internal governance and risk management frameworks to validate that D&I considerations are being integrated thoroughly across the business.
5. **Non-financial misconduct**
   Internal audit must assess the effectiveness of whistleblowing policies as they become critical in ensuring NFM incidents can be detected, reported, and escalated appropriately. Training needs and employee awareness must also be considered as part of internal audit reviews with specific reference to the risk areas identified by the FCA.

To discuss this topic further, please get in touch.

Jessica Sutherland
Director
jessicasutherland@deloitte.co.uk

Sarah Cook
Senior manager
sacook@deloitte.co.uk

05

ESG

Non-financial misconduct

Non-financial misconduct (NFM) in UK Financial Services refers to unethical or inappropriate behaviour that doesn't directly involve financial transactions or monetary gain – this can include harassment, discrimination, bullying, and other conduct issues that negatively impact the workplace environment or the firm's culture. The Financial Conduct Authority (FCA) and Prudential Regulation Authority (PRA) have increasingly focused on NFM in recent years, viewing it as a key indicator of a firm's culture and governance, which can ultimately affect its ability to meet regulatory obligations and treat customers fairly.

Five things you should know

- In September 2023, the FCA and PRA published consultation papers (CP23/20 and CP18/23 respectively) on measures to improve diversity and inclusion in regulated firms, as well as strengthening expectations regarding how firms should manage allegations of NFM.
- In the first half of 2024, the FCA issued an NFM survey to wholesale firms in the insurance, insurance intermediary, banking and broking sectors, requesting information relating to incidents of NFM in these firms between 2021 - 2023. The data collected included the volume and type of NFM incidents, methods of detection and the actions taken to address these incidents within firms.
- In May 2024, the House of Commons Treasury Committee published a report containing responses from HM Treasury, the PRA and the FCA to the recommendations set out in its report following its "Sexism in the City" inquiry. This included interesting points raised concerning the use of non-disclosure agreements (NDAs), NFM, diversity data reporting and target setting and whistleblowing. The regulators are considering their responses to the points raised.
- Regulatory focus is likely to intensify in the coming years. An FCA policy statement responding to its consultation is not expected until the second half of 2024, and it is likely that we will see more detailed guidance and potentially new rules specifically addressing these issues – it is also possible that some of the bolder proposals may be softened or dialled down in response to feedback.
- To ensure compliance with regulatory expectations, firms are going to need to show that they are taking NFM seriously. They may need to focus on implementing more robust reporting mechanisms and demonstrating (with evidence) how they are proactively addressing cultural issues. In many circumstances, the firm's response is likely to require, or be assisted through, the instruction of experienced, independent and qualified third-party support.

Five things internal audit should do

1. **Code of conduct compliance**
   Internal audit should undertake a review of their company's code of conduct and ethical standards, and consider how adherence to these are monitored, managed and reported.
2. **Whistleblower policy**
   Assessing the design and effectiveness of the whistleblower policy in reporting and addressing non-financial misconduct should also be considered. Reviewing the process for investigating whistleblower reports and the subsequent actions taken by management should also be within scope.
3. **Training and development**
   Consideration should be given to evaluating the adequacy of training and the development of programmes related to ethical conduct and the company's values.
4. **Fair treatment and equal opportunities**
   Internal audit may wish to assess their organisation's commitment to fair treatment and equal opportunities for employees from diverse backgrounds, and review how the business ensures that non-financial misconduct does not disproportionately affect any particular group.
5. **Culture assessment**
   Non-financial misconduct could be considered as part of a wider culture assessment, evaluating the commitment across the organisation towards ethical behaviour, and the promotion of a positive organisational culture, as well as how these commitments translate to actions.

To discuss this topic further, please get in touch.

Richard Storey
Director
rastorey@deloitte.co.uk

Conduct risk

Motor finance discretionary commission

Customers in financial difficulty

Consumer understanding

Pricing and value

06

Conduct risk

Motor finance Discretionary Commission Arrangements (DCA's)

On 11 January 2024, the Financial Conduct Authority (FCA) announced its intention to review historic motor finance commission arrangements and sales practices (between 6 April 2007 to 28 January 2021). The FCA is using its powers under S166 of the Financial Services and Markets Act 2000 (FSMA) across several firms to help inform its conclusions over the size and scale of customer harm, and the actions firms will be required to take to redress customers.

As part of these announcements, an immediate pause (up to 25 September 2024) to FCA complaint handling rules, specifically for complaints relating to DCA's, was announced[1]. At the same time, the Financial Ombudsman Service (FOS) published its final and leading decisions on two DCA complaints relating to two major motor finance providers, which were both upheld in favour of the customer[2] .

Five things you should know

- Whilst further guidance is not expected until September 2024, the FCA and Prudential Regulatory Authority (PRA) have been engaging with firms through: the submission of information requests; reminding firms of the importance of maintaining adequate financial resources to support any potential remediation that may be due[3]; and emphasising the need for firms to robustly challenge their assumptions and consider the full range of stress outcomes related to motor finance commission arrangements.
- Firms have experienced an increase in court claims in this area. Decisions are also awaited from the Court of Appeal on three test cases[4] and a Judicial review[5].
- Given the unprecedented actions taken by the FCA, combined with the precedent set by the two leading FOS cases and ongoing legal action, there is a distinct possibility that some form of remediation will be required.
- Firms must continue to take pro-active steps to assess their historic exposures and the scale of their impacted portfolio in preparation for the FCA's conclusions. Firms facing challenges over data availability should understand where they have gaps in their data, and demonstrate how reasonable steps have been taken to fill these using other sources.
- Whilst the temporary pause on DCA complaints is in place, firms need to ensure that they are complying with FCA rules and requirements for both DCA and non-DCA complaints.

Five things internal audit should do

1. **Programme plan and governance**
Many firms will find that establishing a programme is critical to identify and plan key activities, engage stakeholders, assess resources required and manage key risks and dependencies. Internal audit should consider providing assurance over this programme with a focus on rigour and evidence of decision making.

2. **Historic exposure assessment and analysis**
Functions should consider the robustness of the DCA programme methodology used to identify key impacted time periods, agreements and customer cohorts, to ensure that the inclusion or exclusion of key parameters is sufficiently rationalised and aligns to regulatory requirements, expectations and guidance.

3. **Data integrity**
Functions should challenge the data gaps identified by management and ensure steps are taken to resolve these data gaps. Internal audit could also undertake file reviews to support the firm's data analysis activities, to understand how the firm's approach to DCA's operated at an individual customer level and to validate potential exposures.

4. **Compliance with PS24/1.**
Assurance activities over a firm's compliance with PS24/1 during the (temporary) pause period should be considered with a specific focus on the design and operating effectiveness of the firm's arrangements for; identifying, segregating and responding to both DCA and non-DCA complaints in line with expectations, with appropriate oversight.

5. **External audit**
Internal audit should be cognisant of activities in flight by the firm's external auditors in support of financial provisioning, and ensure that this is considered when scoping for internal audit reviews in this area.

1 PS24/1: Temporary changes to handling rules for motor finance complaints | FCA
2 financial-ombudsman.org.uk/decision/DRN-4188284.pdf and Decision Reference DRN-4326581 (financial-ombudsman.org.uk)
3 Dear CEO letter: Maintaining adequate financial resources (fca.org.uk)
4 Motor finance test cases against Close Brothers and Firstrand head to Court of Appeal (cityam.com)
5 Barclays mounts legal challenge over car finance claim | Business News | Sky News

To discuss this topic further, please get in touch.

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

Priyesh Kotadia
Associate director
pkotadia@deloitte.co.uk

06

Conduct risk

Customers in financial difficulty including vulnerable customers

UK households' financial resilience has weakened following the pandemic and the increasing cost of living. The June 2024 Bank of England financial stability review highlighted that three million households are set to see mortgage payments increase by on average 28%. Renters remain under pressure from higher payments, and whilst inflation is easing, consumers continue to be impacted by cost of living factors.

Consequently, customers in financial difficulty, and the treatment of vulnerable customers remains a key focus area for the Financial Conduct Authority (FCA). The recent fine of a major UK Bank demonstrates the implications of failing to deliver good customer outcomes and having inadequate risk management in place.

Five things you should know

- In May, the FCA fined one UK Bank £6.2 million over the treatment of customers in financial difficulty, citing breaches of Principle Three (adequate risk management) and Principle Six (treating customers fairly). This fine was accompanied by sizeable investment in corrective action and customer redress.
- The fine was imposed as a result of the identification of multiple failings including: payment arrangements without appropriate affordability assessments; inappropriate forbearance measures; and issuing default notices and final demands where accounts had the potential to be brought up to date.
- PS24/2 takes effect from 4 November 2024 creating rules from previously issued guidance during the covid pandemic. The changes include a focus on: early intervention; wider consideration of forbearance options including the waiving and / or suppression of interest; communications and sign posting to third-parties; and a change to the reference of vulnerable customers.
- The FCA are conducting a thematic review into how firms are acting to understand and respond to the needs of customers in vulnerable circumstances. The findings will be shared by the end of 2024. The review will look at how firms treat customers, including those in vulnerable circumstances and will assess, amongst other things, skills and capabilities of employees.
- Given identification of vulnerability can be challenging, and also subjective, we are seeing increased exploration of the use of advanced analytics and artificial intelligence (AI) by first line teams to help spot vulnerability in customers through behavioural modelling, however such tools remain in their infancy and are not widely adopted.

Five things internal audit should do

1. **PS 24/2**
   Internal audit may want to consider a review of any roll out activity for PS24/2, for example looking at any gap analysis completed or impact assessment to ensure the business has identified the right changes. The scope should include a review of policy updates to assess that they reflect expectations of the new rules, as well as considering any changes made by the business to conduct monitoring over these changes
2. **Internal audit coverage of customer outcomes**
   In light of Consumer Duty expectations, internal audit should consider whether the business has sufficient visibility of outcomes and areas of risk of harm through its assurance and oversight activity, and should tailor the internal audit plan accordingly. Specific consideration should be given to the outcomes being received by different customer groups, including those that are vulnerable.
3. **Effectiveness of first and second line assurance**
   Internal audit may want to consider the extent to which first and second line assurance activity (both QA and outcome testing) reflects any changes in a lender's understanding of harm as a result of Consumer Duty. Reviews of assurance activity could also consider methodology areas such as sample size, frequency, coverage of product, customer profile and stage of arrears.
4. **Conduct management information (MI)**
   Functions should review the design and operational effectiveness of conduct MI, governance and oversight, considering learnings from the recent fine and requirements from PS24/2. Consideration should be given to the extent to which MI can effectively monitor the risk of harm in the collections journey and demonstrating appropriate outcomes.
5. **Vulnerable customers**
   Outcome testing continues to highlight missed vulnerability and insufficient tailoring of services. As such, internal audit should consider the changes a firm has made to its approach to product and service design, to assessing value, and its overall monitoring of the outcomes of vulnerable customers across the product lifecycle and in specific customer journeys. As part of this work, internal audit should consider performing outcomes testing.

To discuss this topic further, please get in touch.

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

Louise Gardie-Lloyd
Associate director
lgardielloyd@deloitte.co.uk

06

Conduct risk

Customer understanding

The Financial Conduct Authority's ("FCA") Consumer Duty should be embedded into organisational culture with a clearly documented causal chain of potential consumer harms / outcomes, processes, controls and monitoring activity in place. There are four outcomes documented in the Consumer Duty, and the consumer understanding outcome is the outcome focused on how firms communicate with their consumers throughout the lifecycle of a product.

The benefit of good communication across a product lifecycle is that informed customers are more likely to choose products and services that best meet their needs and consequently firms are less likely to deal with poor customer outcomes or complaints if they get this right.

Five things you should know

- The FCA expect consumers to be given the information they need, at the right time, presented in a way that enables consumers to understand the product they hold, how it works, its benefits, risks and costs, to be able to make good decisions. Firms are expected to act in good faith by avoiding the design or delivery of communications that exploit consumers' information asymmetries and behavioural biases; and also test communications to mitigate the risk of their own perception bias. As such, firms should have a documented strategy and framework that helps them to deliver effective communications with adequate oversight.
- Firms should consider appropriate communication styles and channels. Communications should meet the needs and reading age of the product target market and be tailored to the different segments within. The design of the communication should be informed by the channel used i.e. written, verbal and digital. For example, ensuring the font size on digital communications can be read on mobile phones if customers are using an application web-based service.
- The content of communications should be clear such that customers understand what the product means to them in terms of risk, eligibility, cost (including commissions), features, benefits and restrictions. Additional considerations should be made for more complex products and / or customer profiles.
- The timing of communications should minimise customer harm. For example, if eligibility and benefits are clear and succinct in a sales communication, then customer harm could be mitigated at the initial source. Product events that trigger customer eligibility restrictions or costs should be communicated in advance. Finally, where customers need help, e.g. claims or financial difficulty, the ask of them should be clear, with optionality, so they can provide comprehensive information to support firms in providing customers with good outcomes in times of need.
- Where customer communications are undertaken by a third party, firms need to influence the quality of communications. Specifically, Outsource Service Providers (OSPs) should align to the communications standard of the regulated firm.

Five things internal audit should do

1. **A strategy and framework to support delivery of customer outcomes**
   Internal audit should assess the design and operating effectiveness of the framework in place to deliver good customer outcomes. The framework should comprehensively document the causal chain i.e. the firm has identified potential customer harms, as well as processes and controls designed to mitigate them, and testing / monitoring to assess customer harms.
2. **First line testing of customer communications across different channels and customer groups**
   Functions should assess the adequacy of the customer communications testing programme considering all stages of the product and customer lifecycle, the sufficiency of the data / MI obtained from testing to enable analysis of customer outcomes, and the insights drawn and actions taken as a result.
3. **Governance and oversight of communications**
   Internal audit should assess whether there is evidence of sufficient senior manager leadership, challenge and oversight of the data from the customer understanding framework, and if there is evidence of reporting / escalation of poor customer outcomes at the appropriate governance fora.
4. **Oversight of third-party customer communications**
   Functions should consider assessing the monitoring and oversight controls in place to ensure that customer communications made by third parties are appropriate and align to the regulated entity where necessary.
5. **Assessing communications**
   When working in this area, internal audit should ensure that adequate consideration is given to different communication channels and customer groups.

To discuss this topic further, please get in touch.

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

John Lonen
Director
jolonen@deloitte.co.uk

06

Conduct risk

Pricing and value

The Financial Conduct Authority's (FCA) Consumer Duty sets the standard of care firms should give retail consumers. It's four outcomes are a suite of rules and guidance setting more detailed expectations of a firm's conduct.

The specific focus of the price and value outcome rules is on ensuring the price the customer pays for a product or service is reasonable compared to the overall benefits. Value needs to be considered in the round and low prices do not always mean fair value.

Five things you should know

Firms should have a documented framework in place that enables them to assess the price and value of a product and act where potential customer harms are identified. The framework should prioritise five key focus areas:

- **Price and commission** – the price must be reasonable compared to the overall benefits (the nature, quality and benefits the customer will experience considering all these) and costs incurred by the firm (production, operational and delivery).
- **Service, features and benefits** – there should be an assessment of the service, features and benefits including any limitations. For example, if the price of advice is inclusive of annual reviews, is there evidence that reviews are being performed with customers; or where add-ons are sold with core insurance policies, is there evidence of customers using those add-ons.
- **Costs** – the reflection of costs of production, servicing, delivery and commissions received and paid to partners should be proportionate to those incurred by customers and the service provided. The FCA have previously found that the prices paid by customers are often higher than production and delivery costs which are directly linked to high-level of commissions within the distribution chain.
- **Closed book products** – The FCA recognises that the price and value outcome cannot be so easily applied to existing contracts. The rules are linked to the original contractual terms of products and services and the contractual terms may be vested rights. For example, firms do not need to repeat their underwriting of customers for insurance or credit purposes. That aside, existing products or services should not exploit consumer lack of knowledge and/or behavioural biases to enable: unfair prices to be charged; complex pricing; or terms that make it harder for customers to assess value. Firms should also consider whether significant changes to the benefits of a product or service should affect the price.
- **Data and monitoring** – insight should be based on an analysis of appropriate evidence, an objective view of value across different customer groups (including vulnerable customers), an understanding of the wider market and internal product comparison. For example, firms should assess whether different products have different charges, fees and prices with sufficient evidence of a clear difference in benefit to customers.

Four things internal audit should do

1. **Price and commissions**
   Internal audit should consider assessing the controls in place across the distribution chain to ensure partners receive appropriate commissions as well as limiting excessive remuneration / commissions.
2. **Price and value frameworks**
   Functions should ensure they are assessing the design and effectiveness of price and value frameworks, and whether there is sufficient data-led assessments of a product's fair value, with adequate customer, service, features, benefits, costs and product segmentation.
3. **Closed book**
   For functions that haven't already, an assessment of the approach to closed book products is worthy of consideration. The review should assess the control framework in place to ensure that the ongoing remuneration / commissions received on a product, operational costs, and customer utility equates to ongoing value.
4. **Data governance and oversight**
   Internal audit should consider assessing whether the data used to assess and monitor price and value on an ongoing basis is robust and timely to enable risk owners to rely on it and inform decision-making. This should include consideration of different customer groups, including vulnerable customers, and whether they are receiving value from the product and service.

To discuss this topic further, please get in touch.

Lyndsey Fallon
Partner
lfallon@deloitte.co.uk

John Lonen
Director
jolonen@deloitte.co.uk

Digital risk and change

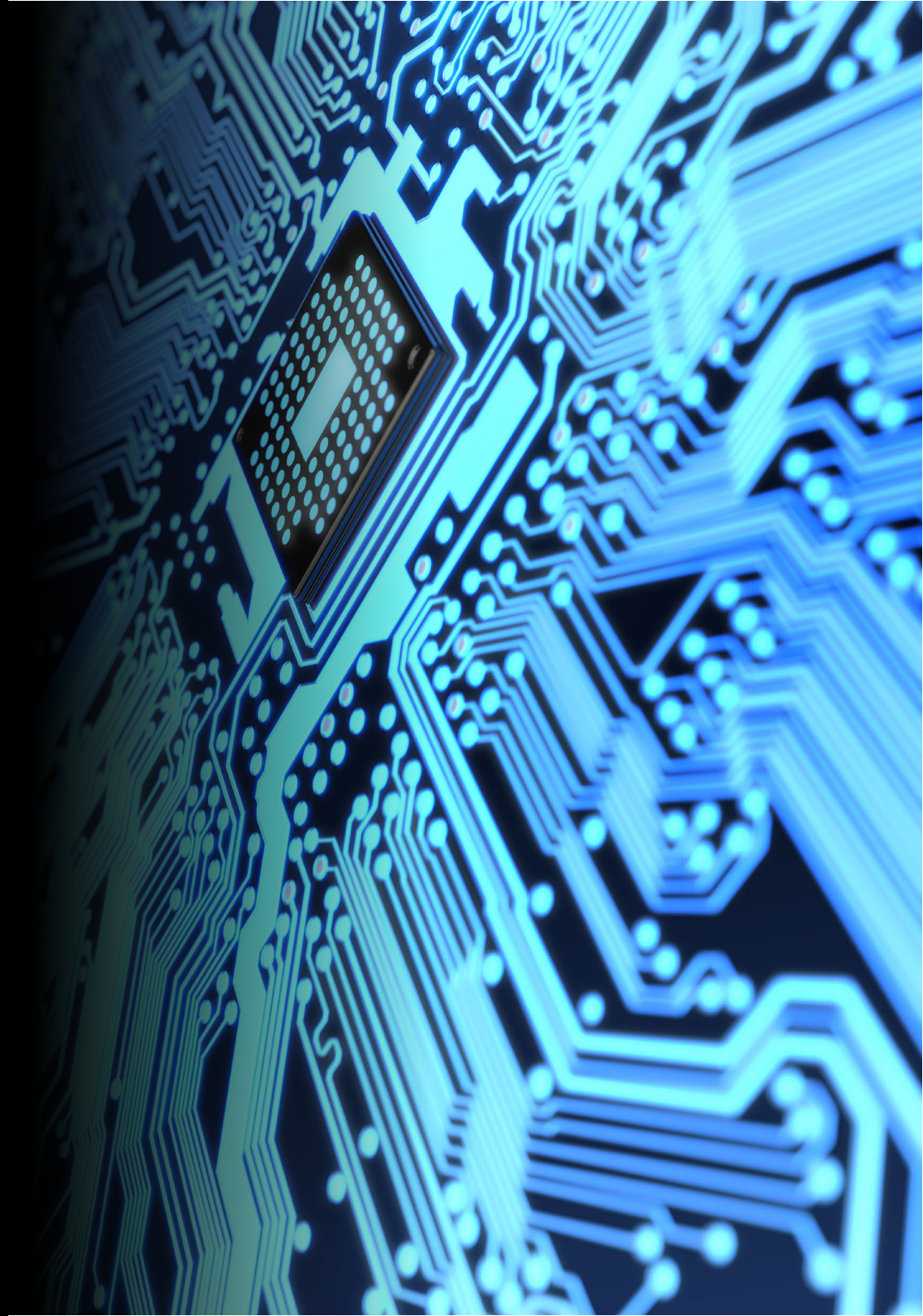
Operational resilience

DORA

Technology and digital governance

Technology transformation and change assurance

Generative artificial intelligence



07

Digital risk and change

Operational resilience

With the deadline for implementation of the Prudential Regulatory Authority (PRA) Supervisory Statement SS1/21, Operational Resilience: Impact tolerances for important business services rapidly approaching, most firms will be in full flight implementation. Firms should also be starting to think beyond 31 March 2025 to the transition to business as usual. Early planning will help to realise efficiencies and synergies more quickly as a firm's approach is refined.

Five things you should know

- The Financial Conduct Authority (FCA) published a webpage in May 2024 setting out their insights and observations for firms as they look to the 31 March 2025 deadline. This includes observations relating to important business services (IBS), impact tolerance, mapping and third parties, scenario testing, vulnerabilities and remediation, response and recovery plans, governance and self-assessment, embedding operational resilience and horizon scanning.
- Several observations made by the FCA highlight a lack of consideration both in terms of breadth and granularity of the topics in question. There is also repeated emphasis of the need for firms to continue to mature their approaches over time, rather than seeing 31 March 2025 as the end-point.
- With this in mind, and as project teams are disbanded, the transition to business as usual will require careful consideration to ensure that the firm's approach continues to develop. Foundational to this will be clarity around ongoing ownership, roles and responsibilities.
- All firms, but especially those who started the journey toward compliance at a later date, should have taken a risk-based approach towards compliance and should have a clear plan with well understood timelines to achieving compliance and to developments beyond this point.
- Part of the transition to business as usual will be the transferral of routine tasks such as the execution of the routine reassessment of IBS following both time and event-based triggers. Firms should ensure that the cadence of these reviews is clearly defined, planned and resourced for and appropriately communicated through governance.

Five things internal audit should do

1. **Dedicated and embedded assurance**
Beyond 2025, internal audit functions should consider how best to get both breadth and depth of their assurance coverage through both dedicated reviews and embedding resilience considerations in other planned audits.

2. **Transition to business as usual**
Internal audit should consider assessing the adequacy for provisions to support transition to business as usual including clear definitions of roles and responsibilities across relevant stakeholders and with adequate ongoing oversight.

3. **Benchmarking**
Internal audit functions who understand how their firm's approach to operational resilience compares to peers will be able to add significant value in helping their firm to refine their approach to ongoing compliance in a proportionate way, aligned to the marketplace.

4. **Management information (MI)**
The importance of management information, post the implementation deadline will become critical as metrics and data are challenged and refined. Internal audit should consider a review of the adequacy of the MI, its alignment to risk appetite, its ability to support decision making as well as the adequacy of proposed actions for management to take where triggers are breached.

5. **Third parties**
Assurance of operational resilience is intrinsically linked to third party risk management. Internal audit may wish to undertake a review specifically focussed on the operational resilience aspects of key third parties including the tracking of any remediation the firm has required by third parties to undertake, consideration of substitutability and exit arrangements.

To discuss this topic further, please get in touch.

Sarah Black
Partner
sarahblack@deloitte.co.uk

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

07

Digital risk and change

DORA

Implementation of the Digital Operational Resilience Act (DORA) is now ramping up ahead of full entry into force on 17 January 2025. By this date, firms will need to be able to demonstrate the operational resilience of their critical or important functions (CIF), ensuring that the technology, as well as the third-party information communication technology (ICT) service providers which support the delivery of these functions, have been mapped and are aligned to the firms' expectations of resilience provision.

The scale and complexity of the DORA remains a challenge for many firms and reinforces the need for a comprehensive and joined-up approach to successfully embed the requirements across a business. Additionally, firms are grappling with designing and operationalising efficient operating models and reporting mechanisms which synthesise different resilience capabilities and functions to address both DORA requirements and that of other resilience regulatory regimes.

Firms should be looking to execute on a DORA strategy which reflects their size and complexity to achieve proportionality against resilience capability. Strategies should also clearly signpost how firms will be managing remediation activity, and the justification, which extend beyond the regulatory deadline. The Digital Operational Resilience Act (DORA) | Deloitte UK

Five things you should know

- **Critical or important functions** – the consistent identification of these functions, at a sufficiently granular level, continues to present challenges to firms, particularly around the treatment of internal, 'enabling' services and how to reconcile different definitions of critical services and functions.
- **Scale and complexity** – with further draft legislation having been recently published, firms should ensure they have appropriate plans in place to ensure they will be compliant in good time. Material changes to the draft legislation are considered unlikely.
- **Programme management** – the breadth of DORA requires firms to bring together ICT risk management, third party risk management (TPRM), incident and crisis management as well as other resilience functions to support implementation and onward transition into business-as-usual activity.
- **Regulatory expectation** – the supervisory approach is yet to be defined for what regulators will regard as leading practice and the approach they will take for oversight and inspection. Firms should remain alert for developments in this area.
- **Third-party involvement** – significant effort will be required to uplift the oversight of third parties for firms within the scope of DORA as well as contractual elements, conducting regular testing and obtaining robust assurance will be critical.

Five things internal audit should do

1. **Gap analysis and action plan documentation**
With many firms having completed their gap analysis, the focus of Internal audit should shift to assessing the adequacy of the programme of remediation activity, how this is being tracked, whether the activity is sufficient to address the gaps identified and whether activity will be complete by the deadline.

2. **Governance**
Functions may also wish to examine the governance arrangements for DORA, beyond the remediation programme. This should include consideration of the target operation model for supporting compliance with DORA as business-as-usual including involvement of the correct stakeholders, ownership and oversight.

3. **Mapping**
Internal audit should consider reviewing some of the mapping exercises that have been performed to ensure they are an accurate reflection of the end-to-end processes being considered.

4. **Proportionality**
When reviewing the Digital Operational Resilience Strategy and other relevant documentation, internal audit should consider if the firm has set out clearly, its approach to proportionality, ensuring this is risk-based and takes account of the firm's scale and complexity.

5. **Scenario based testing**
Testing plans should be examined by internal audit to ensure they appropriately cover identified CIF and the ICT services required to deliver these functions. Scenarios should reflect the changing environment of ICT risk, encompassing the current and potential risk landscape.

To discuss this topic further, please get in touch.

Sarah Black
Partner
sarahblack@deloitte.co.uk

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

07

Digital risk and change

Technology and digital governance

The establishment of an effective technology and digital framework represents one of the biggest areas of both risk and opportunity for firms. Optimised frameworks can deliver cost reductions, support management of risks in line with appetite, and enable innovation and delivery of strategic goals. This is particularly important in the cost constrained environment in which most firms currently operate. Recent major global incidents reinforce how important it is for organisations to get this right.

Five things you should know

- **Firms should focus on the visibility and understanding of technology by senior leadership:** With the continued fast paced nature of technological change, even IT practitioners can struggle to maintain an adequate knowledge of the evolving technology landscape. Without a clear understanding and foresight of potential changes, it makes it difficult for boards, executives and senior leadership to effectively challenge on technology strategy, investment and BAU activities.
- **Increased focus on delivering and measuring value from IT is needed:** Boards should continue to challenge Chief Information Officers (CIOs) and Chief Information Security Officers (CISOs) to ensure they can demonstrate effective governance structures are in place, and that the service and performance of these functions are proactively and effectively managed. These teams must deliver value for money to the business and help protect the organisation from technology, digital and cyber risks.
- **Reporting on technology risk can be improved:** The information available to those charged with governance of technology delivery is often insufficient, particularly in key areas like technology risk management and technology risk appetite.
- **Risk management culture and practices can be enhanced:** In many organisations the culture around technology governance is not where it needs to be. Technology practitioners are stretched on day-to-day delivery and matters of governance and risk management may not be given adequate focus. For example, lessons learned from breaches or bypassing of controls, reported by staff, may not be followed up on.
- **There is a lack of adherence to established IT governance frameworks:** The ISO/IEC 38500:2015 standard as well as Control Objectives for Information and Related Technology (COBIT) should be leveraged by functions in their assessments of organisational compliance against established IT governance frameworks. Such frameworks centre around four pillars: strategic alignment (strategic IT planning and organisational structure); IT risk management (risk management structures, policies and processes); resource management (resource planning including capacity and capability; IT third party management) and value delivery and performance measurement.

Five things internal audit should do

1. **Perform a holistic review of technology governance**
Internal audit should consider including a review of technology governance and risk management in their plans. Assurance should focus on key aspects of their technology environment, such as strategy, resourcing and capability, risk management, operating model and organisational structure, value delivery and performance monitoring.

2. **Understand the technology environment and develop a tailored plan**
Internal audit should invest time in understanding the technology environment and the risks within this, in order to best tailor the audit plan to provide appropriate coverage of technology risks.

3. **Understand how the technology risk appetite has been defined and is used for monitoring**
Internal audit must also understand how the organisation is setting technology risk appetite, and how it is then used by the business as a tool to measure risk profile on an ongoing basis.

4. **Technology culture**
Assessing the culture within the organisation (both within and outside the technology department) is another key review for the overall assessment of technology governance, which functions should incorporate in their plans.

5. **Review technology governance on a cyclical basis**
Ensure that reviews of technology governance are considered a key component of the technology audit plan on an ongoing basis. For example, consider rotating coverage against the four core areas:

   - strategic alignment (strategic IT planning and organisational structure);
   - IT risk management;
   - Resource management including third party management;
   - Value delivery and performance measurement.

To discuss this topic further, please get in touch.

Yannis Petras
Partner
ypetras@deloitte.co.uk

Mark Westbrook
Director
markwestbrook@deloitte.co.uk

07

Digital risk and change

Technology transformation and change assurance

We have seen a rapid evolution in modern technology transformation due to the accelerating adoption of agile and Lean Portfolio Management (LPM) methods, uniting a variety of shorter and more strategic initiatives designed to solve emerging business needs.

Driven by the pace of adoption of new technologies such as generative artificial intelligence (GenAI), sustainable technology, and low-code application platforms, the success or failure of strategic initiatives can have a significant impact on the reputation and confidence of internal and external stakeholders.

Internal audit functions in mature environments are playing a pivotal role in assuring the organisation's technology change and transformation portfolio. A one-size-fits-all, reactive approach to assurance over transformation and change is no longer appropriate. Proactive challenge is vital, including through attendance at strategically important change governance boards. Monitoring for the achievement of objectives and key results (OKRs) on critical initiatives means internal audit is not tied to the traditional milestone cadence of projects and programmes.

Five things you should know

- **Strategic alignment and value addition:** We are seeing an increase in alignment of transformation activities with strategic goals in order to enhance organisational coherence and prevent wastage on projects and products that do not add any value to colleagues or customers. Assurance engagement should be across the portfolio and coordinated with business sponsors to add value.
- **Digital transformation and scenario analysis.** There is a high demand from stakeholders to deliver projects more quickly through agile and hybrid methodologies, enabling initiatives to stop, start, and re-focus. This requires conducting a scenario analysis to assess the potential outcome of the changes before they are implemented. Change assurance should assess the effectiveness of the scenario planning and adaptability of the portfolio.
- **Regulatory focus on technology:** In light of recent major global incidents, global regulators are pushing for the control over use of automated workflows for development, testing and deployment. It will be important that internal audit functions maintain a strong understanding of these technologies in order to develop and deliver an appropriate approach to assurance.
- **Government focus on cyber threats:** Upcoming legislation will aim to tackle the growing number of attacks on the digital economy by cyber criminals. The legislation could include powers to proactively investigate potential vulnerabilities in systems. Changes to technology solutions will need to have a tighter focus on resilience and cyber security. Organisations should anticipate an impact on the complexity of change programmes to meet transparency requirements.
- **The role of AI:** Advancements in GenAI are challenging many industries by creating new ways to interact with customers, automating complex tasks, and restructuring roles. The pace of adoption, and the ethical challenges raised by the use of GenAI should be a significant focus for management and assurance providers.

Five things internal audit should do

1. **Change prioritisation and portfolio management**
The internal audit function should challenge the approach to strategic prioritisation and portfolio management to ensure alignment with strategic objectives and regulatory compliance. This should extend beyond discussion in governance forums and should challenge bias, inconsistency, benefits realisation, and unexpected outcomes.
2. **Accountability of sponsors and leaders**
Accountability, decision-making, and financial control should reside at the portfolio level. Assurance over a lean portfolio requires proactive oversight, open structures and evidence of transparency between professionals. Assurance must be part of this structure to provide independent oversight to ensure consistent dialog and challenge from the third line.
3. **Resourcing**
Internal audit should assess the organisation's capacity and capability to execute transformation appropriately and robustly, through operating model and capability assessments, monitoring for overreliance on third-party expertise, 'black box' tools and product-led procurement.
4. **Embedded risk management**
While thematic reviews remain a common practice for change assurance, internal audit should consider a more proactive approach of embedding audit resources within programmes and portfolio to give real-time risk assessment, timely challenge, and value-added feedback.
5. **Measuring value**
Internal audit is becoming increasingly critical in measuring the business benefits from major transformation. For example, by assessing the decision-making criteria for shaping change ahead of mobilisation, measuring key metrics to track progress, and monitoring delivery throughout the life of the initiative.

To discuss this topic further, please get in touch.

Lee Hales
Director
lhales@deloitte.co.uk

Olga Harte
Senior manager
oharte@deloitte.co.uk

07

Digital risk and change

Generative artificial intelligence

Generative artificial intelligence (GenAI), a branch of artificial intelligence (AI), has taken the world by storm and its ability to create original content across various modalities is revolutionising numerous industries. There is a huge opportunity to use GenAI to transform internal audit processes, please see the separate AI topic under the Internal Audit section of this publication. However, the existence of such a powerful tool, if used irresponsibly, can lead to potentially reputation damaging consequences. AI models can generate false information through hallucinations, potentially leading to the spread of misinformation, and the quality of training data used is crucial to avoid biased and/or suboptimal outputs. Firms are grappling with the right level of 'human in the loop' to ensure AI systems are not accountable for decision making. Establishing effective controls is essential to ensure GenAI services are secure, comply with laws and regulation and do not put the organisation's reputation at risk.

Five things you should know

- In response to GenAI risks, regulatory frameworks have been established across the globe. The EU AI Act will have implications for UK businesses with ties to the EU, affecting those with customers in the EU and those developing, deploying, or marketing AI systems in the EU. The EU AI Act introduces a risk-based approach to ensure AI systems respect fundamental rights, safety, and ethical principles.
- The UK Government's planned AI regulation framework aims to promote creativity through the safe use of AI, underpinned by five principles: safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress.
- The Bank of England, Prudential Regulatory Authority (PRA) and Financial Conduct Authority (FCA) have responded to the UK Government's principles-based regulatory approach and are considering areas for further clarification within their regulatory framework, including data management, model risk management, governance, and operational resilience and third-party risks.
- The FCA has highlighted a number of its existing rules and guidance that it views as most critical to address the UK's AI principles. The PRA and Bank of England have confirmed they will run a third instalment of the 'machine learning (ML) in UK financial services' survey to continue their analysis of the financial stability implications of AI/ML.
- Whilst some clarity has been provided on the regulators approach to AI, further rules, guidance and policy statements are due to be released over the comings months.

Five things internal audit should do

1. **AI regulation readiness**
   Firstly, internal audit should understand how the business has assessed and taken action as a result of incoming and anticipated legislation. A project-based approach may be relevant here.
2. **GenAI strategy and governance**
   Aside from regulations, internal audit should consider a review focused on the current state of the risk and control framework for AI. Many businesses have already defined their AI strategy and others have made progress in producing an AI inventory and assessing the current state of the business processes adequacy in light of AI.
3. **AI risk management**
   Internal audit should consider the embeddedness of AI risk within the wider risk management landscape, for example, integration in risk appetite and risk metrics, how AI risk is monitored and reported along with clarity of roles and responsibilities. Many organisations have developed their own AI risk assessment process which can be reviewed.
4. **AI system review**
   Internal audit should consider a review of any significant or high-risk AI system in the live environment. The review focus can include a reperformance of the risk assessment performed by management, sample testing of the effectiveness of AI controls, or focus on whether expected benefits and value are being realised in practice. A regulatory lens can also be applied to the review of an AI system.
5. **Training and competence**
   Internal audit should consider the skills and capabilities within the organisation to manage AI risks including how training has been rolled out to all staff using AI and the embeddedness of this understanding.

To discuss this topic further, please get in touch.

Yannis Petras
Partner
ypetras@deloitte.co.uk

Lewis Keating
Director
lkeating@deloitte.co.uk

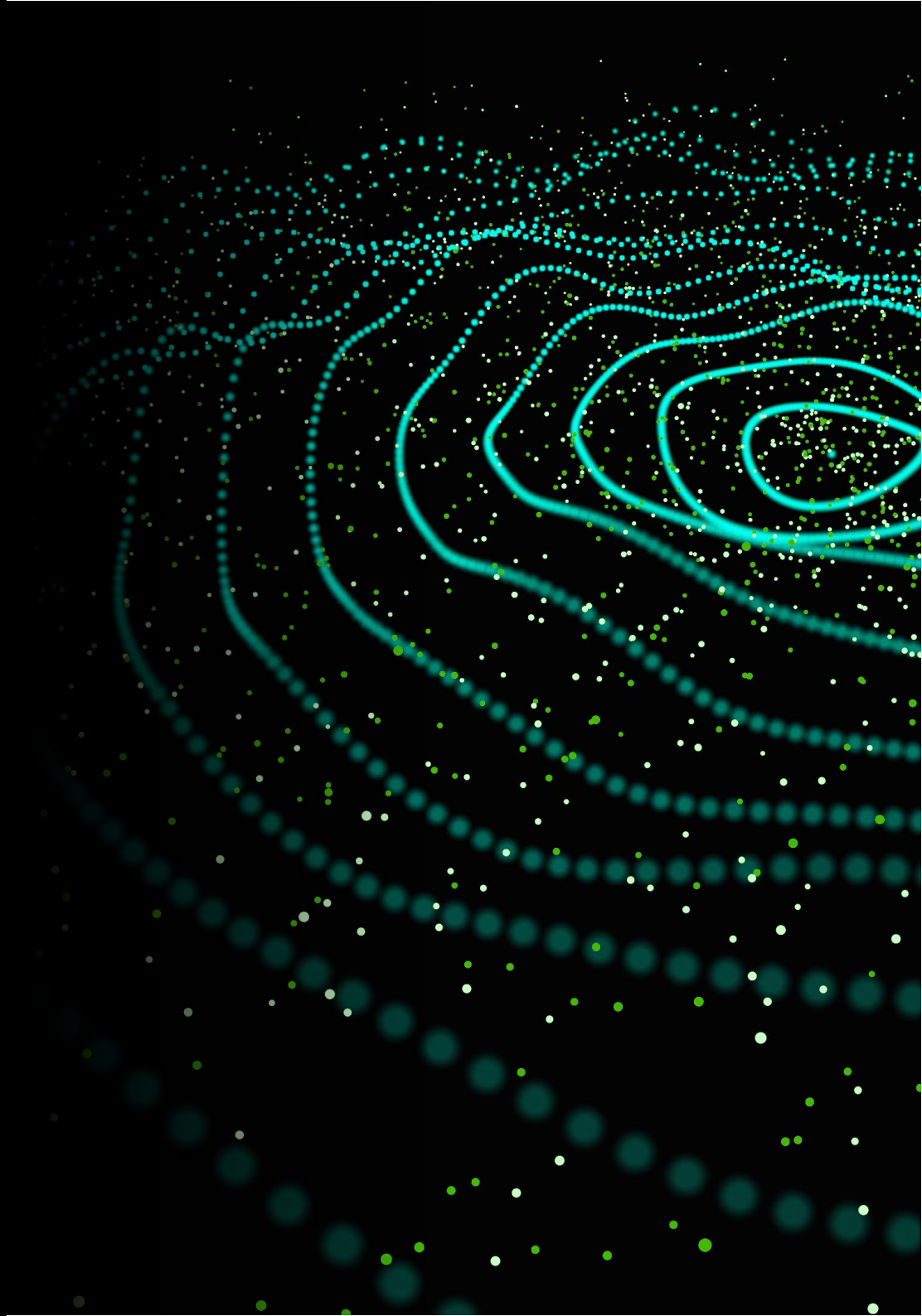
Internal audit

Using generative artificial intelligence in internal audit

Leveraging the new standards

People strategy

Data analytics and process mining



08

Internal audit

Using generative artificial intelligence in internal audit

Generative artificial intelligence (GenAI) represents a groundbreaking type of machine-learning model that focuses on creating new data rather than simply making predictions. Its potential to revolutionise work processes and business data interactions, accelerating operations and uncovering innovative opportunities, has been clearly demonstrated across organisational areas, such as chat bots for customer interaction, virtual assistants, code generation and much more.

For internal audit, the emergence of GenAI presents unparalleled opportunities for functions to enhance efficiency, quality and impact at all stages of the audit lifecycle including risk assessment, audit planning, automated testing, working paper generation, report drafting, audit committee summaries and issue tracking. Additional benefits beyond the lifecycle exist too, such as automated resource scheduling or curated learning paths based on skills gaps. According to our 2024 Chief Audit Executive (CAE) survey, a significant proportion (38%) of functions are planning substantial investments in GenAI within the next one-three years.

Five things you should know

- The adoption of GenAI is a journey: Functions are beginning to explore use cases while simultaneously evaluating technology options and addressing challenges such as: access to large language models, whether on-premises or through hyperscalers and other software-as-a-service providers; data security; and team readiness.
- Balancing risks and opportunities: Organisations, including internal audit functions, will need to assess the risks and opportunities associated with GenAI. The benefit of efficiencies gained from reduced manual effort need to be balanced with the need for appropriate governance and controls over accuracy and accountability of output.
- The way we work will change: GenAI can be used to accelerate routine tasks such as drafting initial audit scopes, creating initial risk and control matrices, compiling standard reports, and tracking of open audit findings, amongst others. This creates space for auditors to focus on higher-level analysis, strategic thinking, and ad hoc problem-solving, leading to a more engaging and rewarding work experience.
- Data governance is increasingly important: The audit team may need to strengthen data governance practices to ensure the accuracy, security, and integrity of the data used by AI systems for auditing purposes. Whilst this is already a focus area, this is often at a low stage of maturity and will need to improve at pace to ensure functions are ready for the impact of GenAI tools and are able to deploy them safely.
- Evolving regulatory landscape: Rapidly evolving regulations around AI usage will require organisations and internal audit functions to play close attention in order to remain compliant across all operational geographies.

Five things internal audit should do

1. **Develop the GenAI aspect of your digital strategy**
Internal audit should determine the potential of GenAI to facilitate achieving broader, functional goals. Existing strategies for digital should extend beyond GenAI to cover other areas of machine learning and existing data management systems. Common areas include report generation, methodology chat bots, audit committee summarisation or quality assurance coaches.

2. **Increase digital literacy**
Internal auditors should engage with learning and development now. Although not everyone needs to become digital experts, being familiar with the terminology and potential of AI tools will accelerate its adoption.

3. **Collaborate with technology teams**
Functions should familiarise themselves with their organisation's stance towards AI, from both data privacy and security perspectives. They should also look to understand the organisation's appetite for shaping existing solutions within its environment.

4. **Clean up your data**
Data quality is crucial for AI's efficacy. As with other departments within the organisation, internal audit should revisit its data management practices and ensure data and records held are up-to-date in order to realise the value AI can deliver.

5. **Establish good governance**
Functions should consider the governance structure required to manage the risks associated with using AI. This should include controls around the use, development, testing, and ongoing monitoring of AI. Again, functions will want to consider how best to align to their organisation's overall approach to AI governance.

To discuss this topic further, please get in touch.

David Tiernan
Director
datiernan@deloitte.co.uk

Nanette Scott
Associate director
nanettescott@deloitte.co.uk

08

Internal audit

Leveraging the new global internal audit standards

The countdown to the new Global Internal Audit Standards (GIAS), effective from 9 January 2025, has begun.

The new Standards are intended to raise the bar for internal audit globally. Functions are noting that the ability to demonstrate conformance is leading to most having to update key artefacts including their charter, methodology, Board and senior management communications, and team training plans. Others are looking to take advantage of the opportunity presented by the Standards to define or reset the function's purpose and longer-term vision, tailored to that of the broader organisation that they serve.

It is crucial that internal audit functions are well-prepared. The time to accelerate and finalise readiness activities is now.

Five things you should know

- **Timely compliance:** Key stakeholders including the Audit Committee, will expect functions to conform or have clear plans to bridge any gaps by the effective date. Some functions have been delayed from starting their readiness activities, either by not sufficiently considering their conformance gaps, or through a need to prioritise plan delivery.
- **Self-assessment at the individual requirement level:** The Standards require functions to perform periodic self-assessments of conformance to the Standards. Detailed self-assessments at the individual requirement level are critical to avoid future conformance issues. We are seeing significant variation in the detail that functions have gone to in documenting self-assessments.
- **Engagement with the Board and senior management:** This will be needed to fully realise the benefits intended by the newer elements of the Standards and will be key to help develop a forward-looking internal audit strategy, with a clear vision, aligned to the broader organisational objectives.
- **Training:** Many functions have already identified gaps around training their people, with plans focused on enhancing the design of ethics-based training and gaining assurance over team members maintaining their CPD. Few functions have plans to provide teams with training on the new Standards more broadly, despite readiness activities typically being performed by a relatively small number of individuals charged with quality or methodology oversight.
- **Future developments:** For UK based organisations the bar is likely to raise further still. In 2024 the Institute of Internal Auditors (IIA) has been consulting on a revised, combined internal audit Code of Practice, which will cover functions in all industries and sectors and is due to launch in September 2024.

Five things internal audit should do

1. **Accelerate your readiness activities**
Functions should be looking to accelerate completion of readiness activities to meet stakeholder expectations in line with the compliance deadline.

2. **Challenge the completeness of your readiness self-assessment and action plan**
Investing time now to clearly document your self-assessment, in line with individual requirements, will ensure action plans are comprehensive. It will also bring added benefits when performing future periodic self-assessments in terms of repeatability and efficiency.

3. **Use this as an opportunity to enhance your function's brand within the organisation**
Forward-thinking functions are using the release of the new Standards to act as a springboard, not only to align on roles and responsibilities, but to enhance internal audit's position, by demonstrating clear relevance to the broader purpose and vision of the organisation.

4. **People agenda key points of consideration**
The below will be hot spots that should be factored into internal audit training programmes, if not included already:
   - Ethics and professionalism
   - Broader education on the requirements of the new Standards
   - Updates / changes to audit methodology resulting from the requirements of the new Standards

5. **Prepare for the UK IIA Code of Practice**
Once released, all functions should read and understand the new requirements placed on them by the new internal audit Code of Practice. Appropriate actions, coordinated with GIAS readiness plans, will then need to be taken to ensure conformance with the new requirements of the Code before its effective date.

To discuss this topic further, please get in touch.

Owen Jackson
Director
ojackson@deloitte.co.uk

Daniel Wright
Senior Manager
daniwright@deloitte.co.uk

To discuss this topic further, please get in touch.

Owen Jackson
Director
ojackson@deloitte.co.uk

Philippa Figueiredo
Senior manager
pfigueiredo@deloitte.co.uk

08

Internal audit

People strategy and coaching in internal audit

As we look ahead to 2025, the landscape of internal audit is rapidly evolving, driven by changes in standards, generative artificial intelligence (GenAI) and increasing demands of stakeholders. Internal audit remains, at heart, a people business, and so alongside digital transformation, there is a compelling need to amplify focus on soft skills including critical thinking, communication, and emotional intelligence. In our recent Chief Audit Executive survey, high performing functions allocate 50-75 hours of training per auditor, yet this is often not fully utilised. This challenge is exacerbated by the increasing prevalence of burnout which almost a fifth of functions identify as a pressing issue for their teams. The growing challenge of attracting and retaining top talent in internal audit further compounds the difficulties faced. As functions look to the coming year, the emphasis on people is paramount, and developing a robust people strategy and coaching framework will be critical.

Five things you should know

- The emergence of GenAI will impact the operational landscape of internal audit. Functions are prioritising the development of their people to complement AI-powered analytics and robotic process automation, enhancing risk assessment and audit procedures. However, these benefits can only be realised with digitally enabled people.
- The digital skills gap has prompted 91% of functions to place a strong emphasis on training and development. We understand that many functions want to do more to develop their people and having a clear people strategy will enable this to happen.
- It's crucial for internal audit to acknowledge the significance of soft skills to develop a workforce adept at navigating technology, while demonstrating empathy and ethical decision-making. This highlights the central role of people in the digital transformation of audit functions.
- High-performing functions embrace the 'learn, do, teach' mindset, creating a culture that values the development and empowerment of people within the internal audit function. The challenge is to maintain this culture of continuous learning and knowledge sharing amidst resource constraints.
- The introduction of the International Professional Practices Framework (IPPF) standards in 2025 underscores the importance of people, requiring internal auditor learning and development plans to be closely linked to internal audit strategy. The challenge is to align the plans with the evolving needs of the internal audit function and the broader business environment.

Five things internal audit should do

1. **Establish a robust forward looking competency framework** that does not focus on short term audit delivery but looks to fulfil all aspects of a function's strategy, encompassing technical proficiency, industry-specific knowledge, and **soft** skills. The framework can be used to drive decision making by identifying skill gaps leading to tailored training programmes, and alignment of individual development plans with the goals of the internal audit function.
2. **Promote a holistic talent development approach** by ensuring annual training plans include technical and soft skills. Encourage cross-functional collaboration through knowledge sharing and offer opportunities for interpersonal skill development. Embrace AI as a way to alleviate staff burnout by automating tasks, providing real-time insights, and enable predictive analytics to identify workload patterns. This allows functions to proactively manage workloads and support employee well-being.
3. **Foster a culture of continuous learning and upskilling** in AI-related competencies. This can empower internal audit professionals to better explore how GenAI can be used a strategic enabler in their operational endeavours.
4. **Incorporate learning activities into the audit plan** including knowledge-sharing sessions, cross-functional training and post-audit debriefs Allocate time and budget for training and coaching, promoting a culture of challenge, iteration, and innovation. This approach develops vital skills for future-ready functions.
5. **Harness people data** for talent development purposes, such as performance metrics, skill self-assessment surveys, and feedback scores. Internal audit professionals can utilise this data to demonstrate the impact of their people strategy, help inform decision-making and derive actionable insights for talent development and succession planning within the function.

08

Internal audit

Data analytics and process mining

Data analytics plays a critical role for internal audit by enabling the detection of anomalies, enhancing audit quality, and improving efficiency through automation. It also helps in identifying trends and providing valuable insights for process improvement.

In the rapidly evolving digital era, the significance of data analytics has become even more pronounced, with 62% of functions identifying it as a key investment area over the next one to three years, according to our 2024 Chief Audit Executive (CAE) survey.

Functions are at different stages of maturity when it comes to the use of analytics. More mature functions are now deploying advanced techniques, including an increased consideration of process mining.

Five things you should know

- Successful implementation of data analytics requires a strategic approach: A clear strategy that focuses on the end goal is key to success. Implementing data analytics, whether basic or more advanced, such as process mining, requires access to appropriate data, skills and knowledge, and the right tools, all of which require the right level of planning for functions to set themselves up for success.
- Consider cost-benefit across the lines of defence before investing: Investment in tooling such as process mining can come with high costs, so it is important for functions to assess the benefit expected before deciding what to focus on first. Collaboration between internal audit and other lines of defence may yield a better return on investment, while also creating a more holistic approach to process improvement and risk management.
- The quality and availability of data is crucial for accurate results: Whilst more advanced techniques, such as process mining can be valuable in revealing hidden insights, the benefit is better realised by functions who have access to the right data.
- Advanced process mining tools are suited to complex business processes: Process mining is an advanced approach to data analytics used to analyse how processes are executed in practice. It can be helpful in identifying bottlenecks and inefficiencies. Organisations with simple processes may not get the full benefit from advanced process mining tools, however, analysing process data is still highly valuable and simpler techniques could be employed using more common analytics tools to achieve the same objective. We have seen functions using more traditional means to analyse data and create process flows in visualisation tools to achieve the same insights but on a smaller scale.
- Maturity levels vary across organisations: Our CAE survey indicated that only 23% of functions were planning to invest in process mining in the next one to three years. We believe this is largely due to the benefit of process mining being realised by mature functions only, compared to those earlier on in their journey who are choosing to prioritise building a strong foundation of analytics first.

Five things internal audit should do

1. **Develop a clear strategy**
   Functions should look to integrate data analytics into their broader internal audit strategy. Considerations should include, how tools can facilitate more efficient and comprehensive audits, and what the function wants to achieve with these technologies.
2. **Focus on data quality and availability**
   Internal audit should work with relevant stakeholders to ensure that necessary data is accessible and of sufficient quality to support data analytics. This may involve collaborating with IT teams to extract and prepare data for analysis.
3. **Invest in suitable tools**
   Functions should consider the technological needs of data analytics and process mining to deliver desired goals. This may involve investing in new software or tools.
4. **Understand the organisation's processes**
   Internal audit should gain a comprehensive understanding of the organisation's key processes, including systems, data sources, and the end-to-end flow of activities. This understanding forms the foundation for effective data analytics.
5. **Training and skill development**
   Internal audit should invest in training and skills development for team members to build expertise in data analytics. This may involve formal training on process mining tools and methodologies, as well as developing data analysis and visualisation skills.

To discuss this topic further, please get in touch.

Owen Jackson
Director
ojackson@deloitte.co.uk

Nanette Scott
Associate director
nanettescott@deloitte.co.uk

Deloitte.